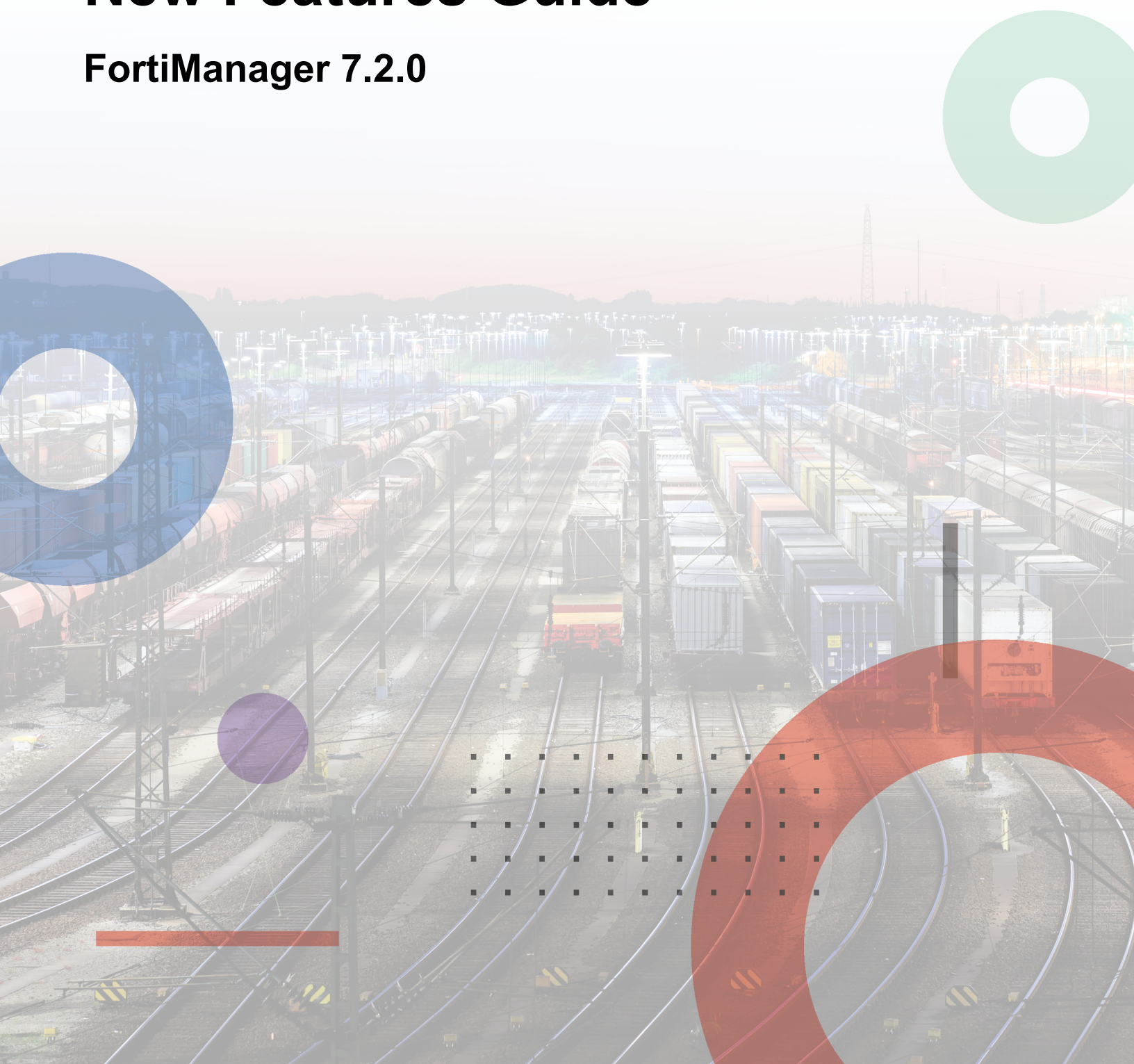
FORTINET

# New Features Guide

## FortiManager 7.2.0



**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO GUIDE**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**NSE INSTITUTE**
https://training.fortinet.com

**FORTIGUARD CENTER**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

April 14, 2023
FortiManager 7.2.0 New Features Guide
02-720-781587-20230414

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2022-04-05 | Initial release of FortiManager 7.2.0. |
| 2022-04-19 | Added:<br>• FortiManager-HA automatic failover enhancement on page 211. |
| 2022-04-22 | Added :<br>• Additional filters available for IPS sensors on page 184<br>• IPS template combines configuration for global "IPS Global" and per-vdom "System IPS " / "IPS Settings" on page 59<br>• IPS administrators have visibility on each IPS profile on page 114<br>• Monitoring page for the IPS on-hold signatures on page 186 |
| 2022-05-10 | Added:<br>• FortiManager updated integration with NSX-T on page 203. |
| 2022-05-11 | Added :<br>• IPS admin install preview for multiple FortiGate devices at once shows the CLI configuration to be installed on each target device on page 115.<br>• Improved design for onboarding FortiGate HA clusters to prevent auto-link failure on page 12 |
| 2022-05-12 | Added:<br>• CLI templates have increased visibility for troubleshooting on page 64<br>• Improved CLI templates with validation and preview functions on page 68 |
| 2022-06-28 | Added New firewall admin role with no RW permission on IPS objects on page 216. |
| 2022-08-09 | Initial release of FortiManager 7.2.1. |
| 2022-08-12 | Added Branch configuration using FortiManager Jinja2 CLI templates on page 247. |
| 2022-08-17 | Added:<br>• FortiManager setup wizard improvement with optional firmware upgrade step 7.2.1 on page 224<br>• Unused Policies filter in a predefined time frame to help security teams for audit purposes on page 161 |
| 2022-08-22 | Added:<br>• FortiManager supports push updates via JSON API for dynamic address groups objects 7.2.1 on page 122<br>• Automatic configuration synchronization for the members of the auto-scaling group in Public Cloud in case of scale-out/scale-in events 7.2.1 on page 234<br>• Enhanced object "where used" function 7.2.1 on page 188 |
| 2022-09-14 | Added:<br>• SD-WAN Monitor includes new filter to display unhealthy devices or interfaces only |

| Date | Change Description |
|---|---|
| | 7.2.1 on page 45<br>• Universal Connector MEA added support for Cisco ACI 7.2.1 on page 229<br>• Visibility improvement for auto-scaling clusters 7.2.1 on page 236<br>• Model device initialization enhancements 7.2.1 on page 22<br>• LAN-Edge: Keep VLAN info when cloning FortiSwitch template 7.2.1 on page 95<br>• The Insert Empty Policy operation will insert a new disabled policy above or below, with no interface pair inheritance from the adjacent policies 7.2.1 on page 163 |
| 2022-09-19 | Added FortiManager-VM has been added to the Flex-VM offering 7.2.1 on page 236. |
| 2022-09-20 | Added VM flexible shapes support for Oracle Cloud Infrastructure 7.2.1 on page 237. |
| 2022-09-23 | Added FortiManager supports BYOL installation on managed FortiGate VM 7.2.1 on page 126 |
| 2022-09-26 | Added:<br>• IPS diagnostics page for IPS dedicated admin displays CPU, memory, and performance statistics for FortiGates related to IPS processes on page 117<br>• Fabric Authorization Template automatically provisions and authorizes LAN Edge devices on the managed FortiGates 7.2.1 on page 74<br>• FortiGates with firmware FOS version 7.0 and version 7.2 can be managed under the same FortiManager 7.0 ADOM 7.2.1 on page 128<br>• ADOM version 7.2 supports policy package installation to the lower version of FortiGate on FortiOS 7.0. 7.2.1 on page 130<br>• NAC policy added to policy package 7.2.1 on page 85<br>• Improved FortiSwitch Manager and AP Manager dashboards 7.2.1 on page 132<br>• AP Manager exposes wireless advanced features 7.2.1 on page 77 |
| 2022-10-24 | Added:<br>• Flex-VM Fabric Connector to support flex licensing management from FortiManager 7.2.1 on page 208 |
| 2022-12-22 | Added:<br>• Internet service database version checked for model devices 7.2.1 on page 25 |
| 2023-02-02 | Initial release of FortiManager 7.2.2. |
| 2023-02-21 | Updated FortiManager-HA automatic failover enhancement on page 211. |
| 2023-04-14 | Added FortiManager displays PSIRT information when a vulnerability is detected for managed devices 7.2.2 on page 152. |

# Overview

This guide provides details of new features introduced in FortiManager 7.2. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable.

The FortiManager new features are organized into the following categories:



For a list of all features organized by the version number that they were introduced, see Index on page 244.

# Device Manager

This section lists the new features added to FortiManager for the device manager:



## Device and Groups

This section lists the new features added to FortiManager for devices and groups:

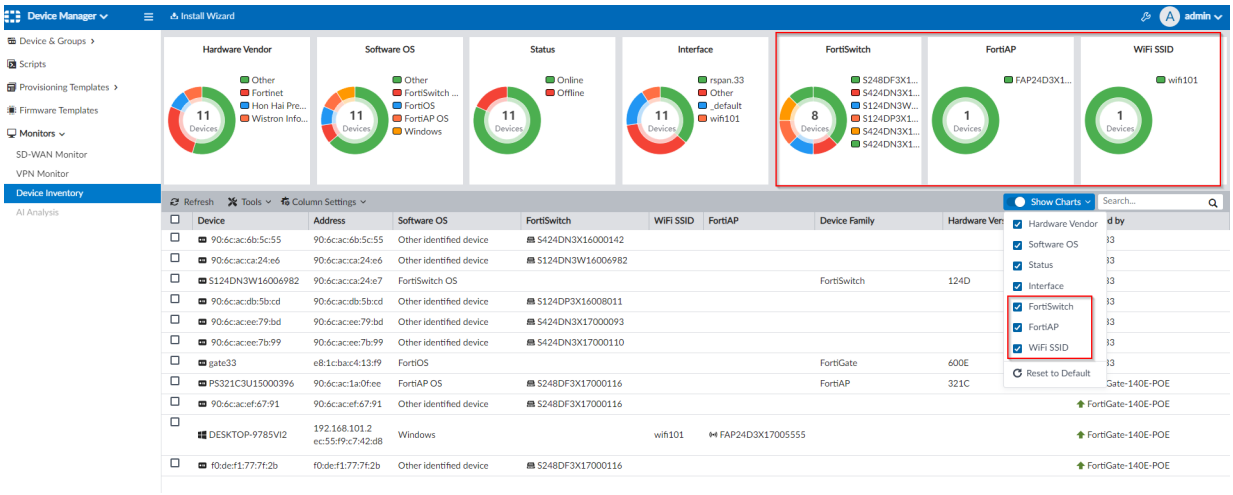


### Device Inventory adds new chart and columns

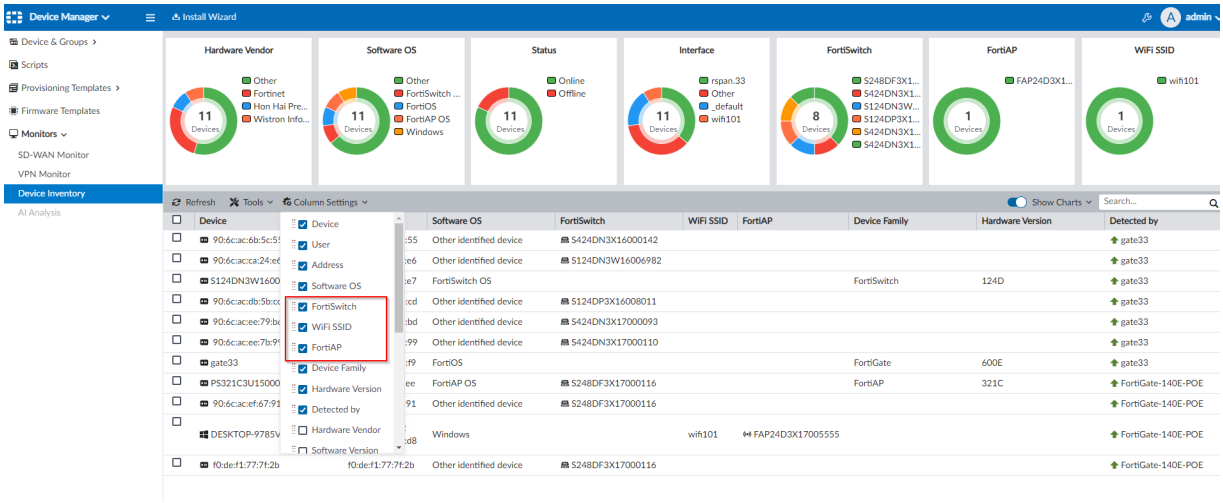
Device Inventory adds new charts and columns to display information on FortiAP, FortiSwitch and WiFi SSID.

**To view the enhancements to the Device Inventory monitor:**

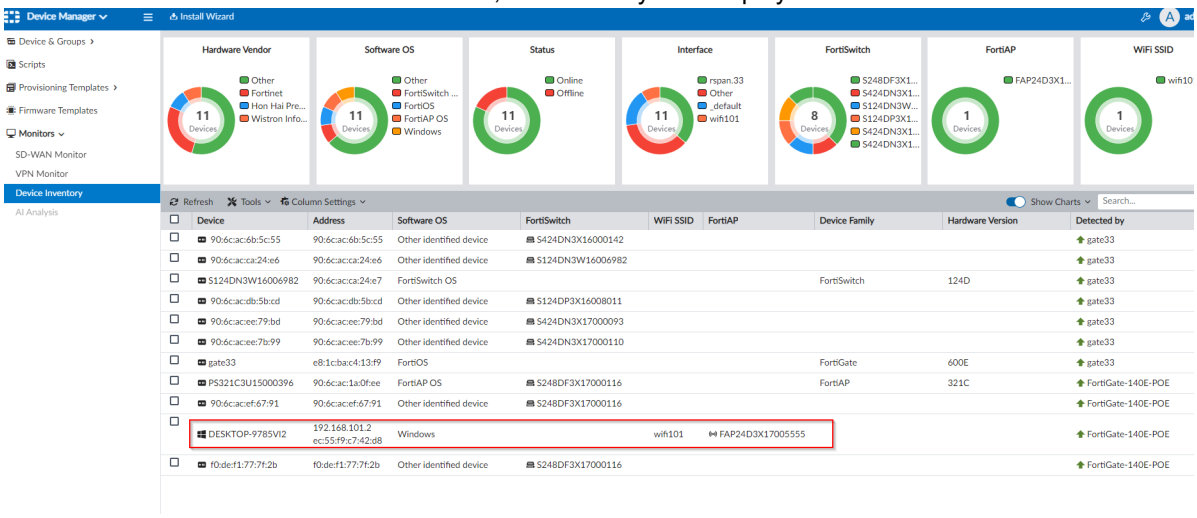
1. Go to *Device Manager* > *Monitors* > *Device Inventory*.
   New charts are added for FortiAP, FortiSwitch, and WiFi SSID, and the charts dropdown list has been updated.



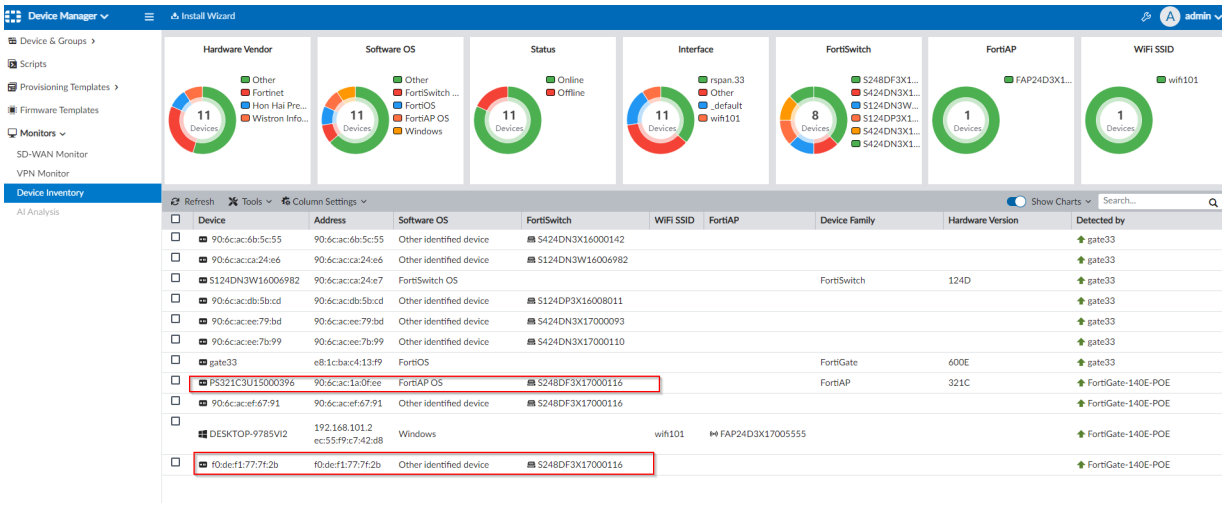

New columns have been added for FortiAP, FortiSwitch, and WiFi SSID.




When a WiFi client is connected to a FortiAP, the inventory item displays the connected WiFi SSID and FortiAP.




When a WiFi client is connected to a FortiSwitch, the inventory item displays the connected to FortiSwitch.

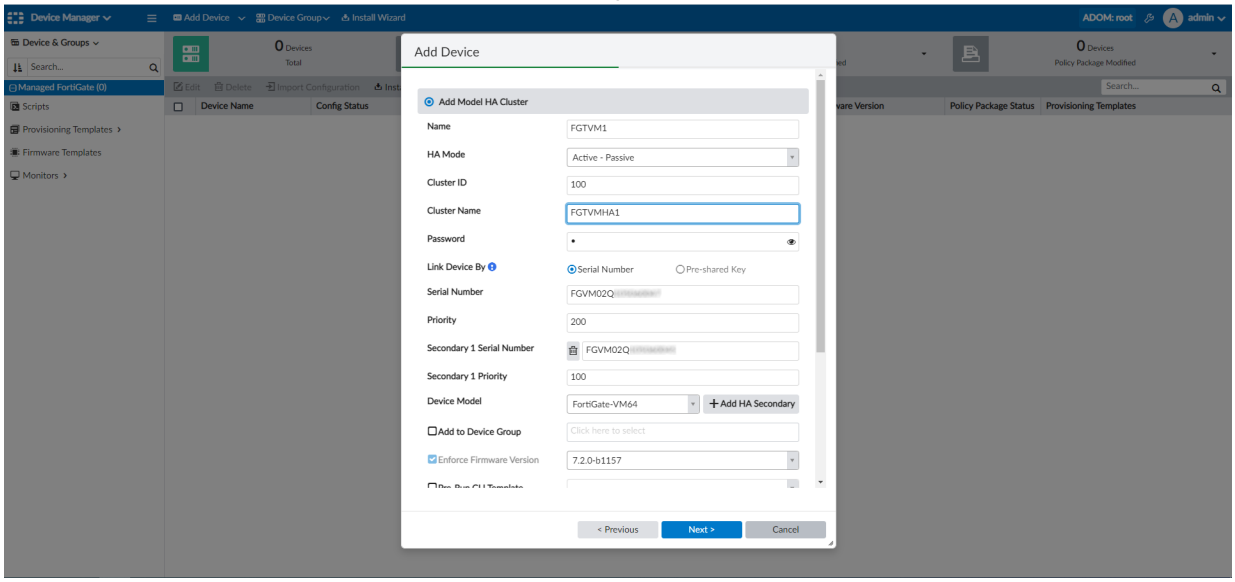



## Improved design for onboarding FortiGate HA clusters to prevent auto-link failure

Improved design for onboarding FortiGate HA Clusters to prevent auto-link failure.

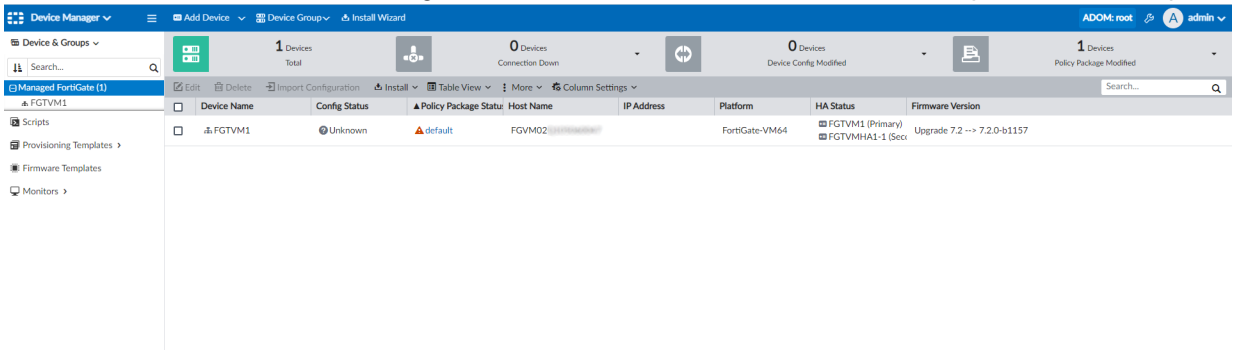
**To add a FortiGate HA cluster using model devices in FortiManager:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Device & Groups*.
3. Click *Add Device*.
4. Select *Add Model HA Cluster*. The Add Device wizard opens.

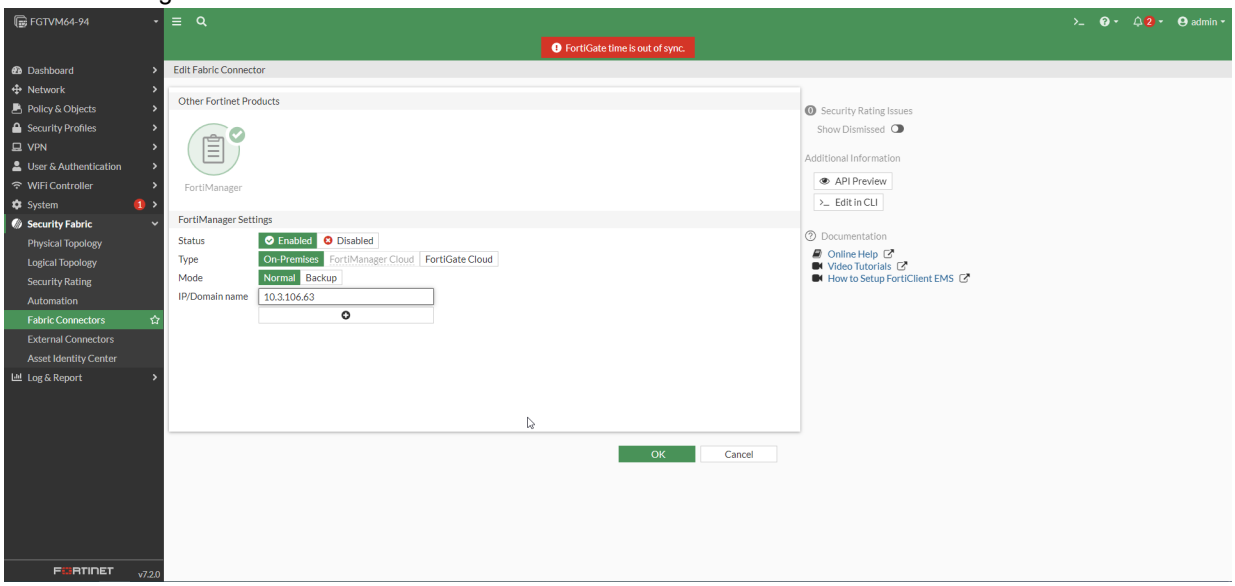



5. Populate the mandatory fields including the *Name*, *HA Mode*, *Cluster ID*, *Cluster Name*, and *Password*.
6. Enter the FortiGate device's *Serial Number*.
7. Optionally, click *Add HA Secondary* to add and configure a secondary cluster device.
8. Configure the remaining settings as needed, and click *Next*.

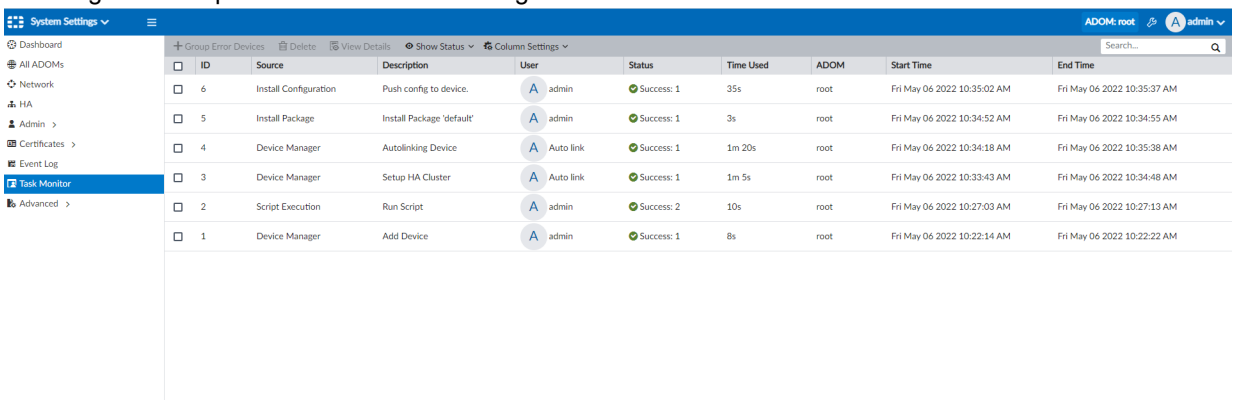
9. After the wizard is finished, FortiManager adds the FortiGate HA cluster in *Device Manager* > *Device Groups*.




10. On FortiGate, go to *Security Fabric* > *Fabric Connectors* > *FortiManager*, and configure the fabric connector using the FortiManager IP for each FortiGate device.

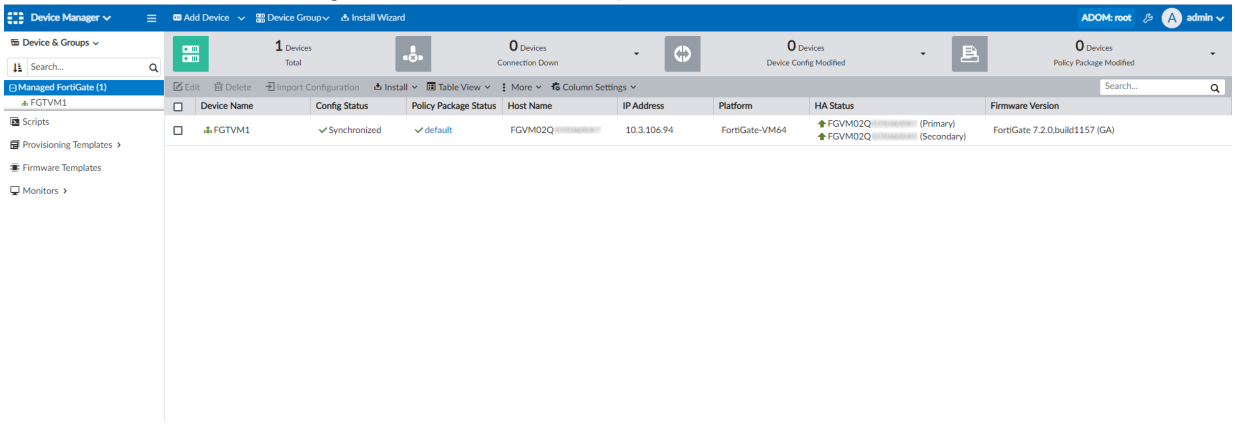



After the FortiManager IP is added to all FortiGate devices, model device auto-linking to real devices begins. The following tasks are performed while auto-linking model devices to real devices:




After auto-link is complete, the HA cluster in *Device Manager* > *Device & Groups* displays additional information

about the HA cluster, including the *HA Status* and *Config Status*.




## Global device dashboard - 7.2.1

A global device dashboard can be used on all managed FortiGates for consistent device monitoring across the organization. This feature is integrated with the add new device and device authorization functions as well.

You can copy device/VDOM dashboards to and from other devices/VDOMs in FortiManager. This allows you to efficiently apply the same custom dashboard configurations on multiple devices/VDOMs instead of configuring each device/VDOM dashboard individually.

If needed, you can customize dashboards individually after they are copied to other devices/VDOMs.

When copying dashboards to and from other devices/VDOMs, the target device's/VDOM's current dashboard configurations will be overwritten.

You cannot copy a dashboard to or from devices on different ADOMs.

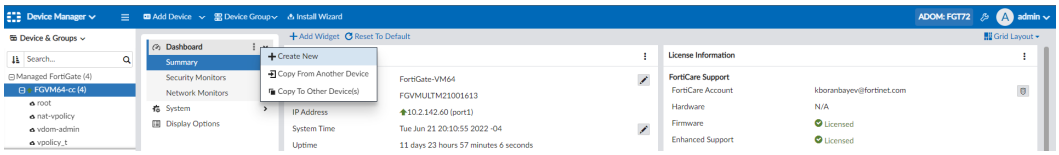
This topic includes:



### To create a device dashboard:

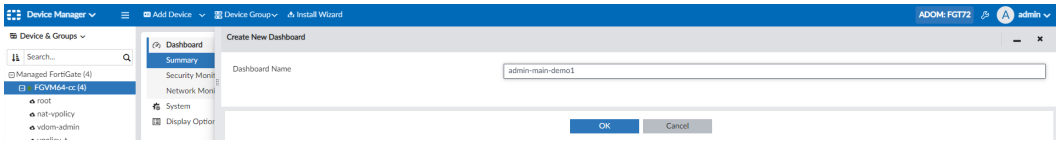
1. Go to *Device Manager* > *Device & Groups*.
2. In the tree of *Managed FortiGate*, select a device or group to create a new dashboard for.

3. From the more options icon for the *Dashboard* menu, select *Create New*.



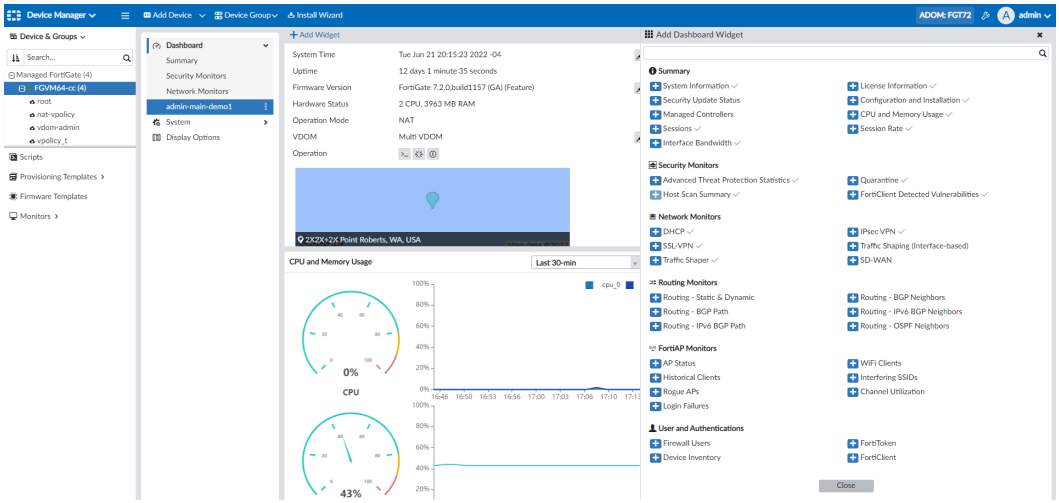

The *Create New Dashboard* pane is displayed.

4. In the *Dashboard Name* field, type a name for the dashboard, and click *OK*.




The *Add Dashboard Widget* pane is displayed for the created dashboard.

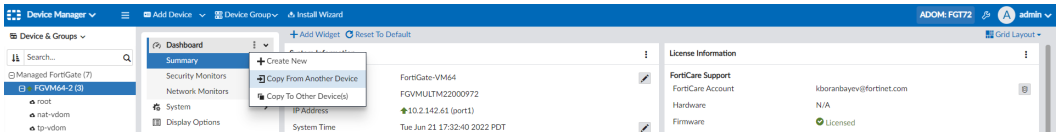
5. Select the widgets to include in the dashboard, and click *Close*.




6. To change the dashboard layout to one, two, or three columns, or to fit the content, click *Grid Layout*.

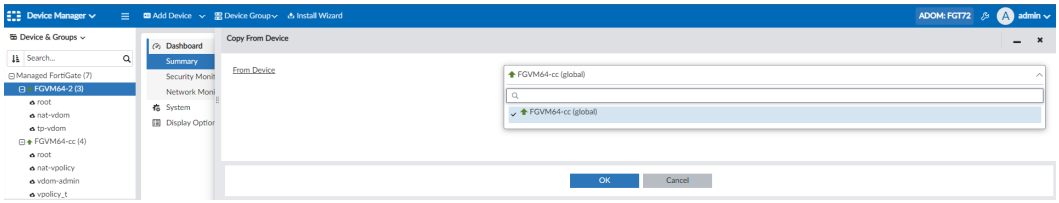
### To copy dashboards from another device:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree of *Managed FortiGate*, select a device or group to copy dashboards to.
3. From the more options icon for the *Dashboard*, select *Copy From Another Device*.




The *Copy From Device* pane is displayed.

4. From the *From Device* dropdown, select a device to copy the dashboards from, and click *OK*.

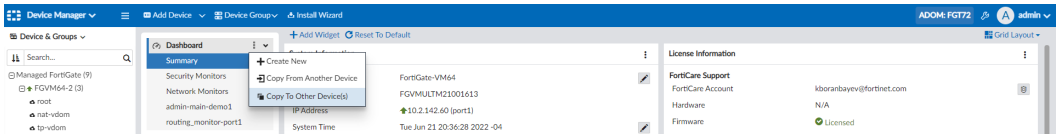


A message asks you to confirm the action.

5. Click *OK*.
   The dashboards are added to the device with the same name and widgets as configured on the device they were copied from.

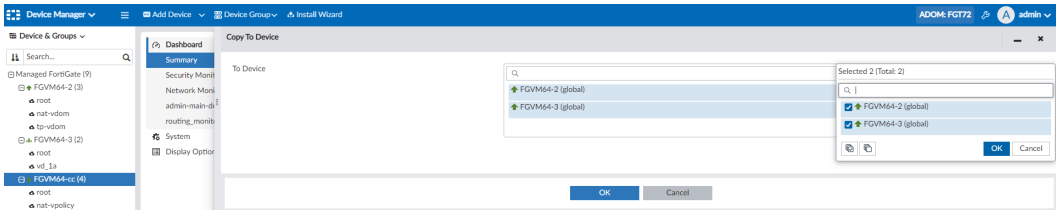
### To copy dashboards to other devices:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree of *Managed FortiGate*, select a device or group to copy dashboards from.
3. From the more options icon for the *Dashboard*, select *Copy To Other Device(s)*.



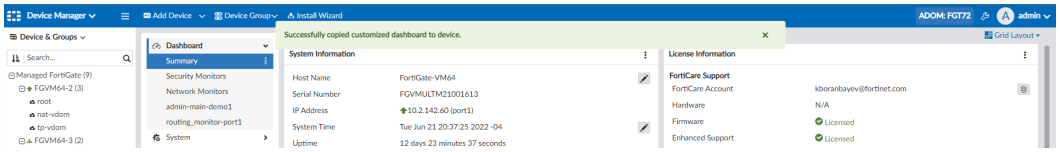

The *Copy To Device* pane is displayed.

4. From the *To Device* dropdown, select the devices to copy the dashboards to, and click *OK*.




A message asks you to confirm the action.

5. Click *OK*.
   A message displays to confirm the dashboards were successfully copied.

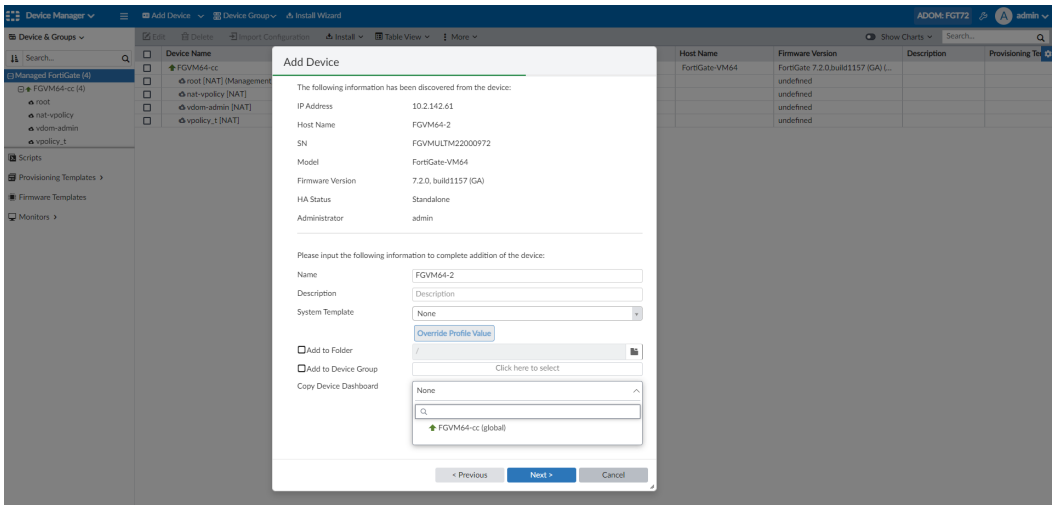



6. In the tree of *Managed FortiGate*, select a device that the dashboards were copied to.
   The dashboards are added with the same name and widgets as configured on the device they were copied from.

### To assign a custom dashboard when adding a new device:

1. Go to *Device Manager* > *Device & Groups*.
2. Click *Add Device*.
   The *Add Device* dialog is displayed.
3. Select the radio button for *Discover Device*, and click *Next*.
4. Complete the device discovery process. See the FortiManager Administration Guide in the Fortinet Docs Library.

5. From the *Copy Device Dashboard* dropdown, select a device to copy the dashboards from.

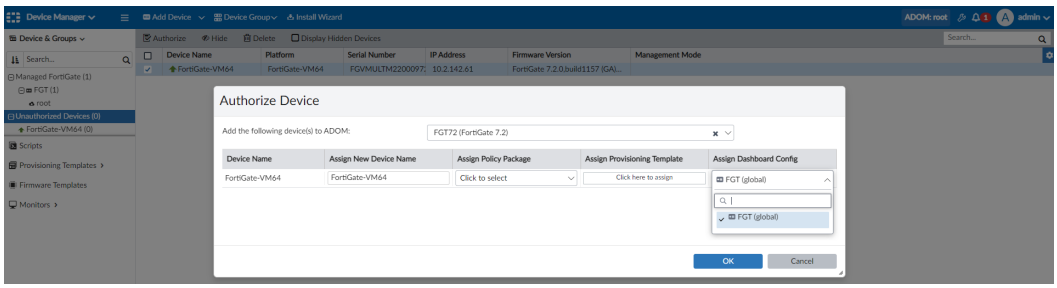



Once the device is added, the dashboards are available with the same name and widgets as configured on the device they were copied from.

The *Copy Device Dashboard* option is also available when using the *Add Model Device* or the *Import Model Devices from CSV* process. See the FortiManager Administration Guide in the Fortinet Docs Library.

**To assign a custom dashboard when authorizing a device:**

1. Go to *Device Manager* > *Device & Groups*.
2. In the sidebar tree, select *Unauthorized Devices*.
3. Select a device, and click *Authorize*.
   The *Authorize Device* dialog is displayed.
4. In the *Assign Dashboard Config* column, select a device to copy dashboards from.

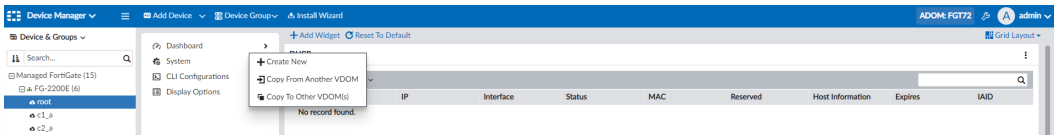



5. Once you have configured the other options, click *OK*.
   The dashboards are added to the authorized device with the same name and widgets as configured on the device they were copied from.

**To create a VDOM dashboard:**

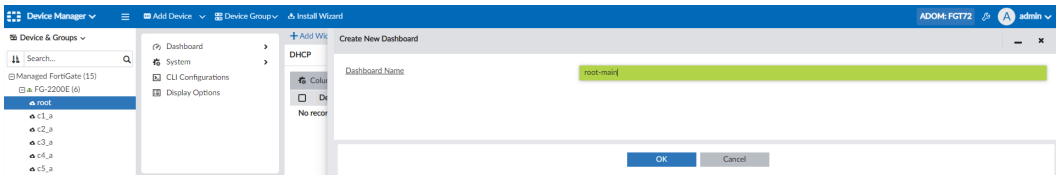
1. Go to *Device Manager* > *Device & Groups*.
2. In the tree of *Managed FortiGate*, select a VDOM to create a new dashboard for.

3. From the more options icon for the *Dashboard*, select *Create New*.



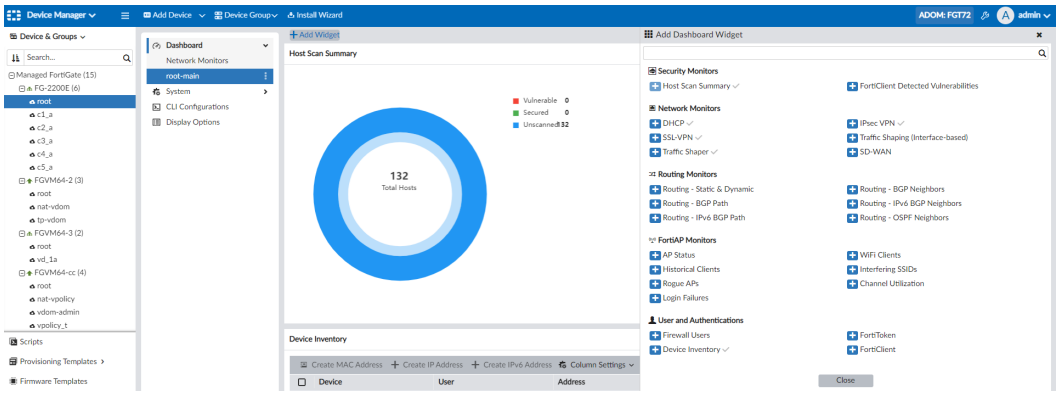

The *Create New Dashboard* pane is displayed.

4. In the *Dashboard Name* field, type a name for the dashboard, and click *OK*.




The *Add Dashboard Widget* pane is displayed for the created dashboard.

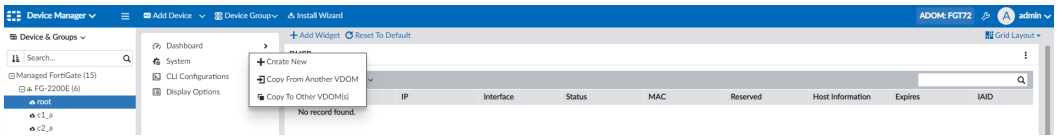
5. Select the widgets to include in the dashboard, and click *Close*




6. To change the dashboard layout to one, two, or three columns, or to fit the content, click *Grid Layout*.

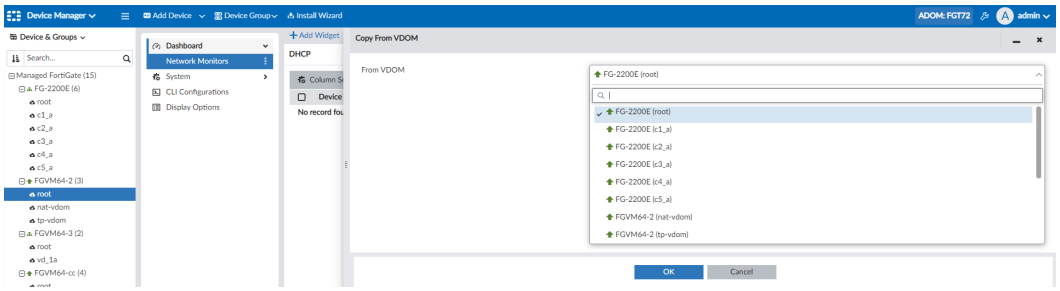
### To copy dashboards from another VDOM:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree of *Managed FortiGate*, select a VDOM to copy dashboards to.
3. From the more options icon for the *Dashboard*, select *Copy From Another VDOM*.




The *Copy From VDOM* pane displays.

4. From the *From VDOM* dropdown, select a VDOM to copy the dashboards from, and click *OK*.

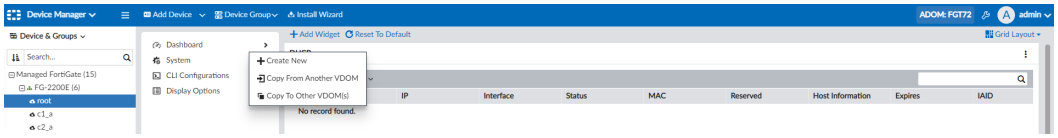


A message asks you to confirm the action.

5. Click *OK*.
   The dashboards are added to the VDOM with the same name and widgets as configured on the VDOM they were copied from.

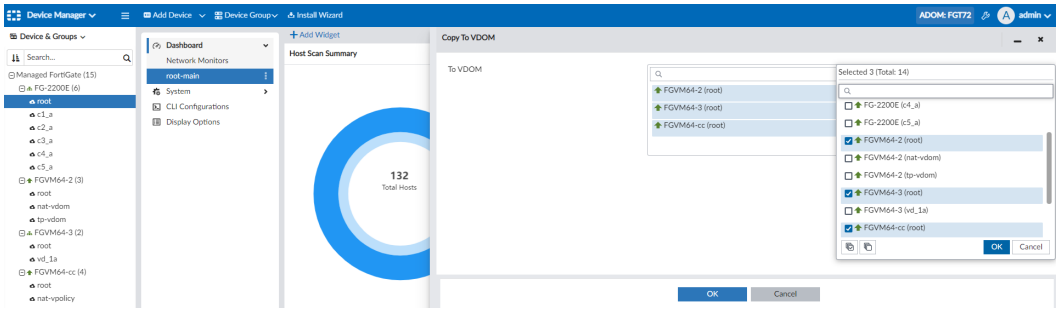
**To copy dashboards to other VDOMs:**

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree of *Managed FortiGate*, select a VDOM to copy dashboards from.
3. From the more options icon for the *Dashboard*, select *Copy To Other VDOM(s)*.




The *Copy To VDOM* pane is displayed.

4. From the *To VDOM* dropdown, select the VDOMs to copy the dashboards to, and click *OK*.




A message asks you to confirm the action.

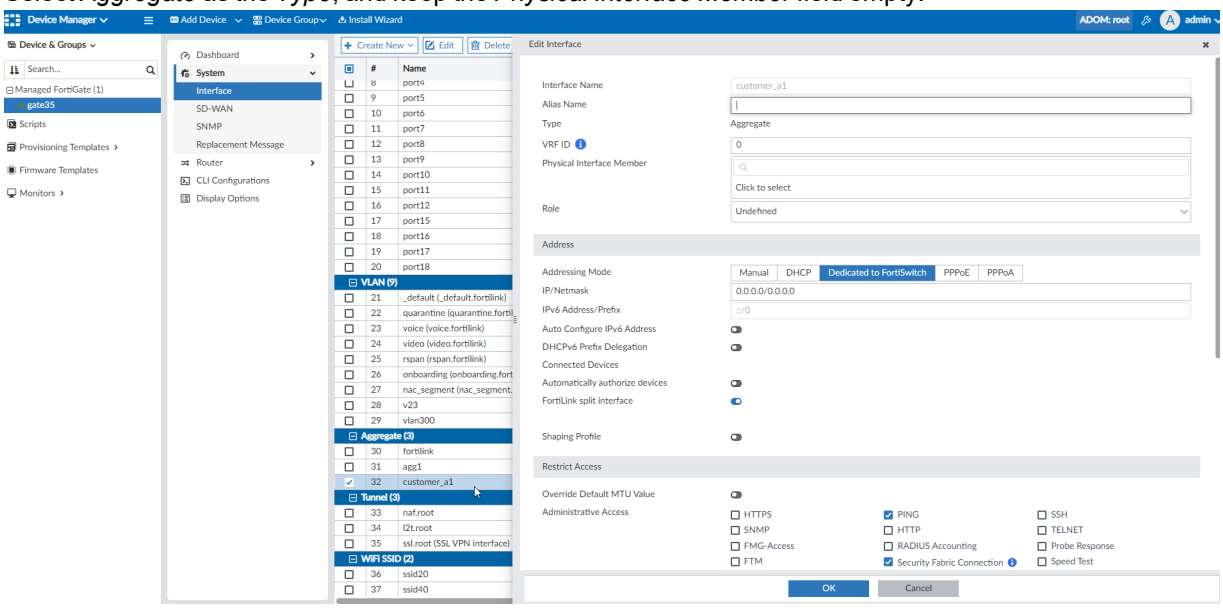
5. Click *OK*.
   A message displays to confirm the dashboards were successfully copied.
6. In the tree of *Managed FortiGate*, select a VDOM that the dashboards were copied to.
   The dashboards are added with the same name and widgets as configured on the VDOM they were copied from.

## Enhancement to aggregate interface allows creation without specifying the interface members - 7.2.1

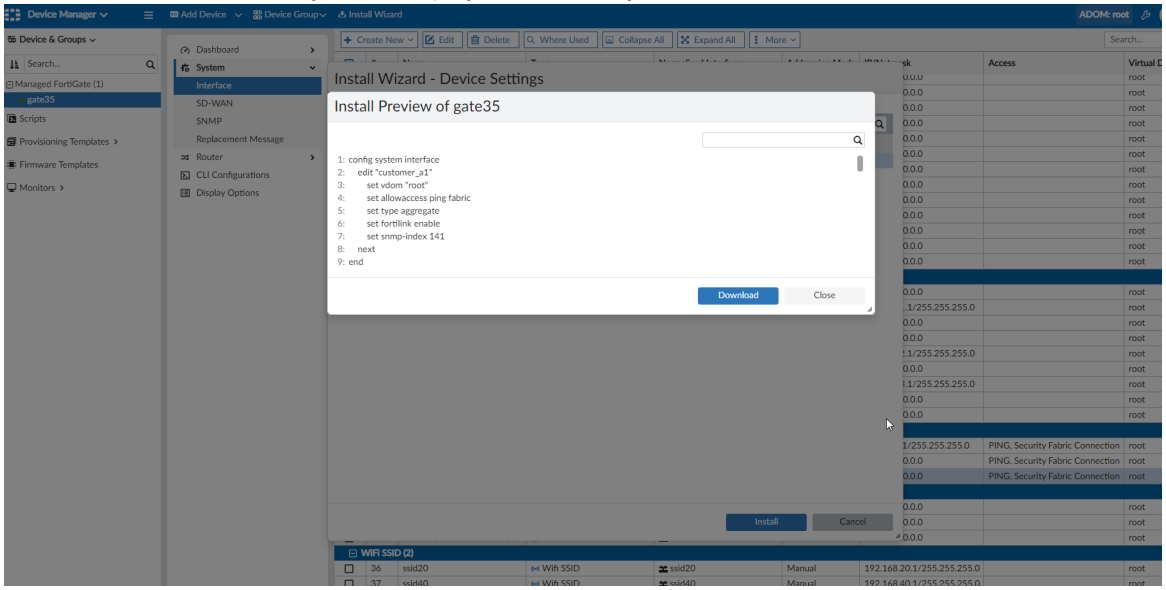
In FortiManager 7.2.1, an enhancement to aggregate interfaces allows creation without specifying the interface members.

**To create an aggregate interface without specifying the interface members:**

1. Go to *Device Manager* > *FortiGate* > *System* > *Interface*, and click *Create New* > *Interface*.
2. Select *Aggregate* as the *Type*, and keep the *Physical Interface Member* field empty.



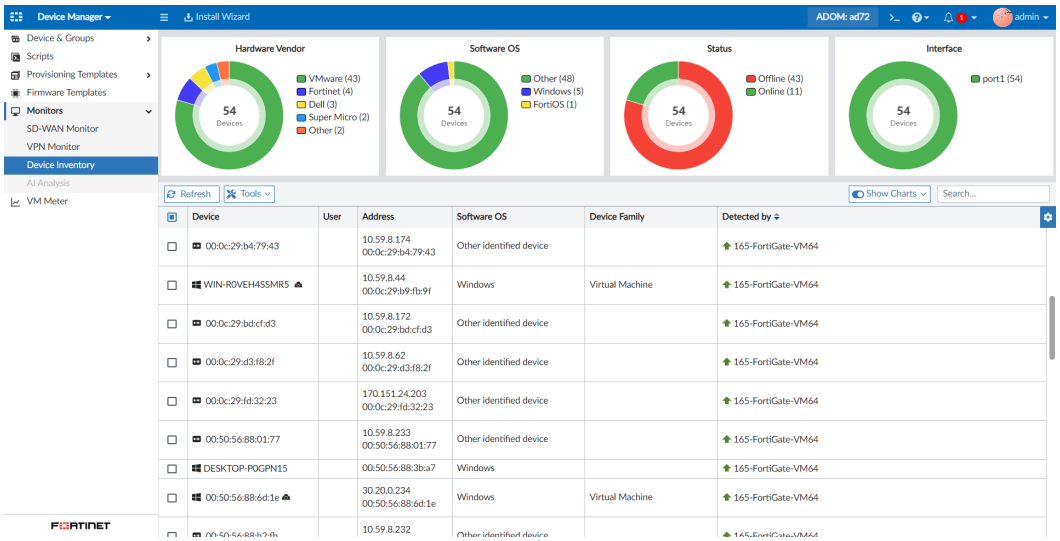

3. Click *OK* to save the interface.
4. After the interface is saved, you can deploy it successfully to FortiGate.



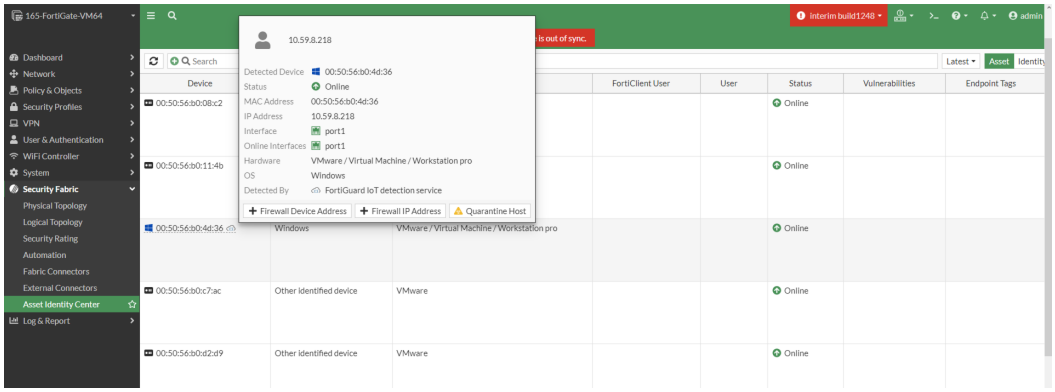

## FortiManager to add IoT devices based on FortiOS Asset Identity Center - 7.2.1

IoT (Internet of Things) devices are now displayed in the FortiManager device inventory monitor.

Go to *Device Manger* > *Monitors* > *Device Inventory*. The IoT devices in the table are indicated by a cloud icon ( ) in the *Device* column.



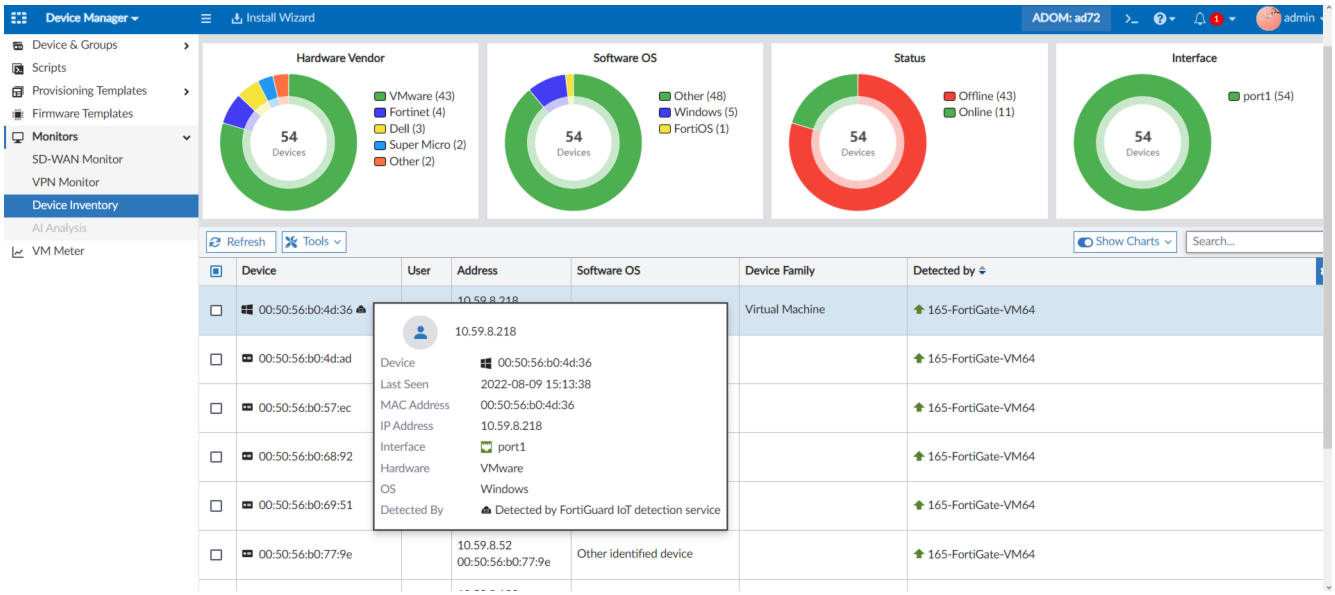

This information is gathered from the FortiOS *Security Fabric* > *Asset Identity Center*. For example:




Collecting this information in FortiOS requires an IoT Detection Service license. For more information, see IoT detection service in the FortiOS Administration Guide.

Similar to the FortiOS GUI, you can mouse over the IoT devices in *Device Manger* > *Monitors* > *Device Inventory* to view detailed information (see below). This includes:

- *Device*
- *Last Seen*
- *MAC Address*
- *IP Address*
- *Interface*
- *Hardware*
- *OS*
- *Detected By*



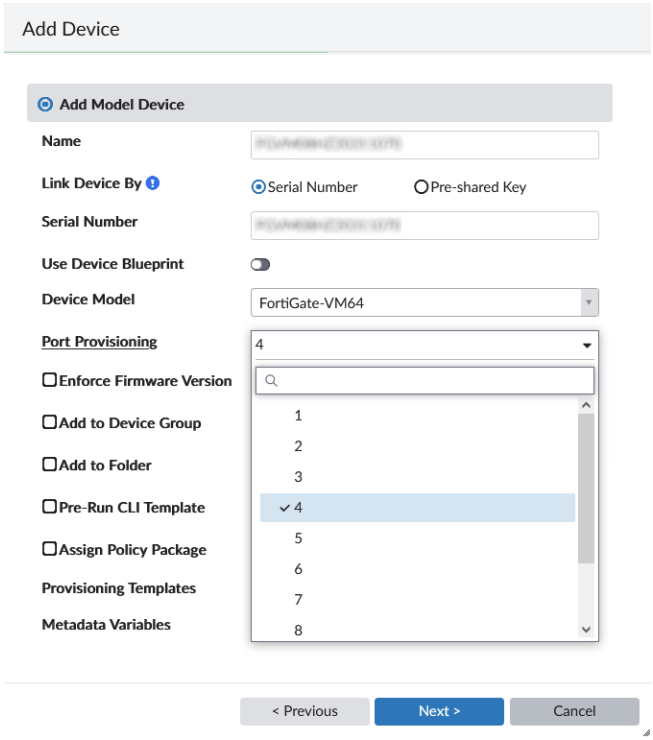

## Model device initialization enhancements - 7.2.1

Model device initialization enhancement can provision the desired number of ports for a VM model and split switch ports for low-end FortiGate appliances.

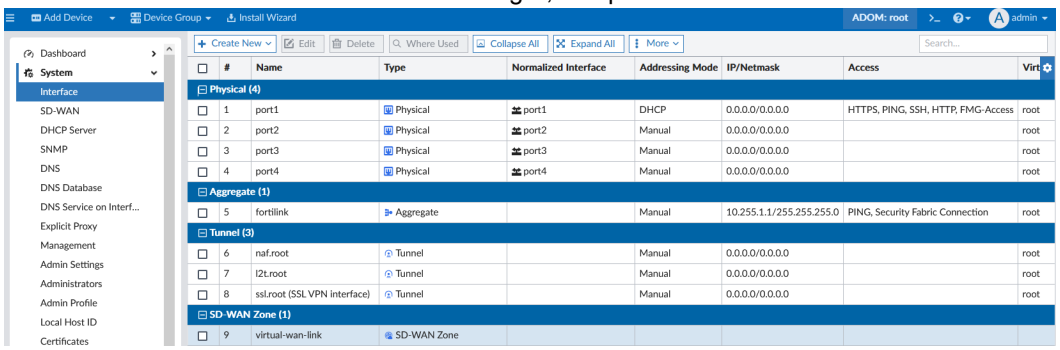
**To add a VM model device and set provisioning ports:**

1. Go to *Device Manager*, and click *Add Device* > *Add Model Device*.
2. Enter the device's *Name* and *Serial Number*.
   When the serial number is entered for a VM device, the *Port Provisioning* field is displayed.

3. Set the number of ports to be provisioned. In the example below, *Port Provisioning* is set to four.

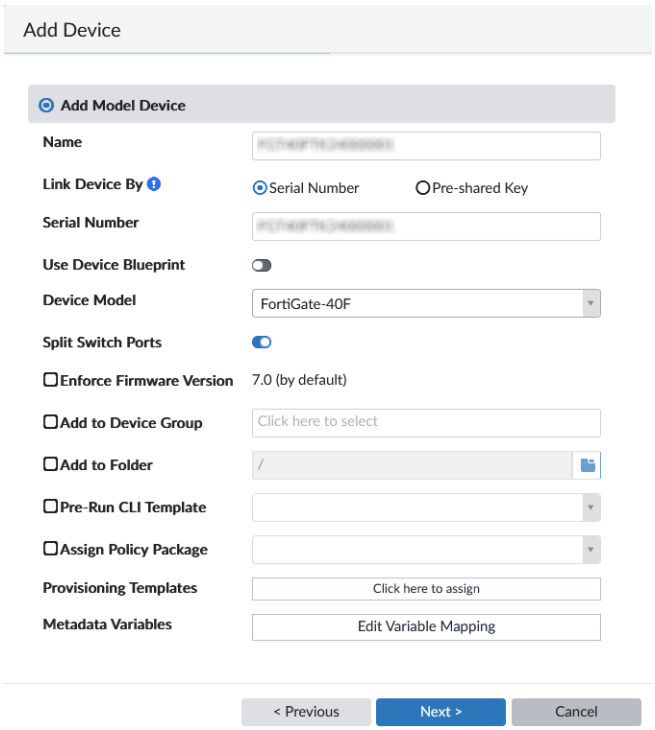



Once this model device is added to FortiManager, four ports are created for the device automatically.

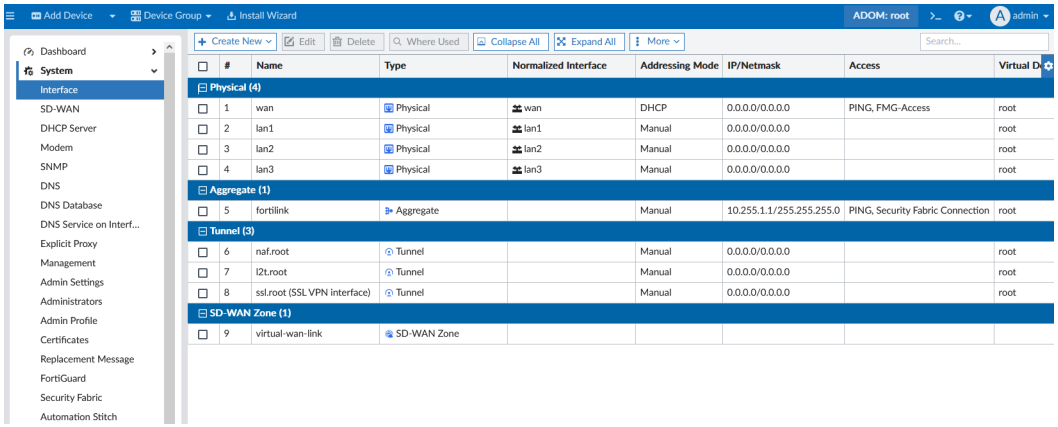



**To add model device (40F, 60E/60F, 80E, 90E, 100E/100F) and set provisioning ports:**

1. Go to *Device Manager*, and click *Add Device* > *Add Model Device*.
2. Enter the device's *Name* and *Serial Number*.
   When the serial number is entered for an eligible device (40F, 60E/60F, 80E, 90E, 100E/100F), the *Split Switch Ports* field is displayed.
3. Set the *Split Switch Ports* field to the *On* position.

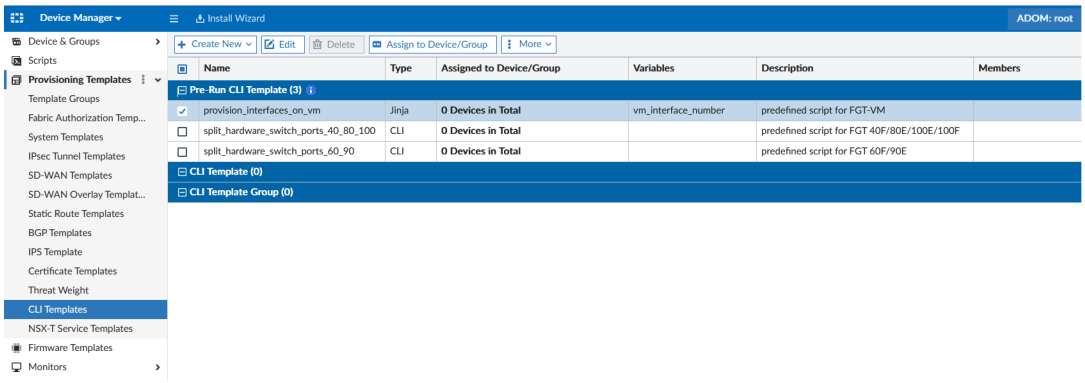



Once the model device is added into *Device Manager*, go to the *System* > *Interface* page. The default virtual hardware switch lan is deleted.




### To view pre-defined CLI templates:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Templates*.
2. Under *Pre-Run CLI Templates*, the following default templates are available:
   - *provision_interfaces_on_vm*
   - *split_hardware_switch_ports_40_80_100*
   - *split_hardware_switch_ports_60_90*




## Internet service database version checked for model devices - 7.2.1

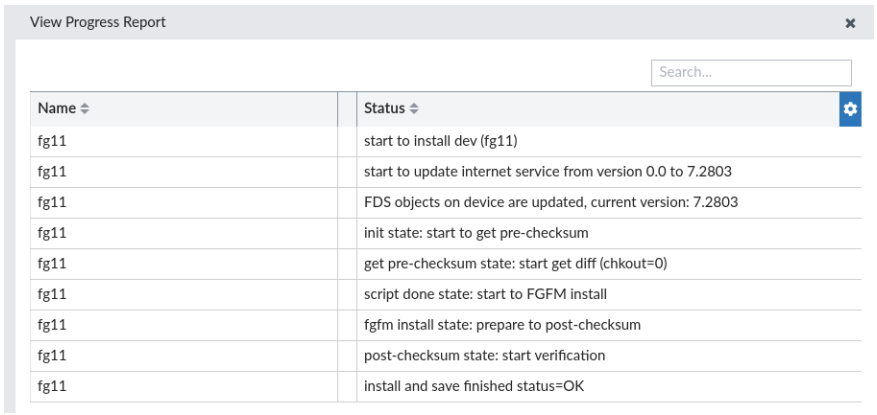
For model devices, FortiManager checks the ISDB (internet service database) version on FortiGates before installing the configuration to the FortiGate. When the ISDB version on the FortiGate is older than the ISDB version on FortiManager, FortiManager triggers an ISDB upgrade on FortiGate before installing the configuration.

If the ISDB version is not updated after three minutes, FortiManager still installs the configuration to FortiGate.

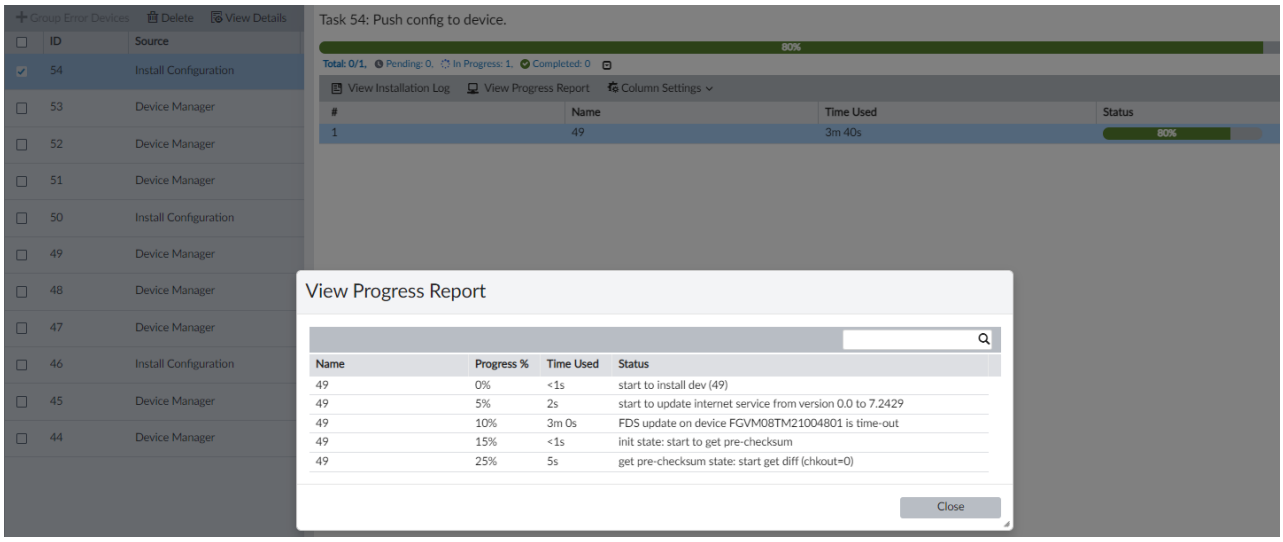
You can observe the behavior in Task Monitor.

**To observe ISDB upgrade behavior:**

1. Go to *System Settings* > *Task Monitor*.
2. Select the *Install Configuration* task, and click *View Details*. The details are displayed.
3. Select a detail, and click *View Progress Report*.
   The following example shows the internet service database version being updated:




If the update to the internet service database fails, the configuration installation still proceeds, for example:




4. Click *Close*.

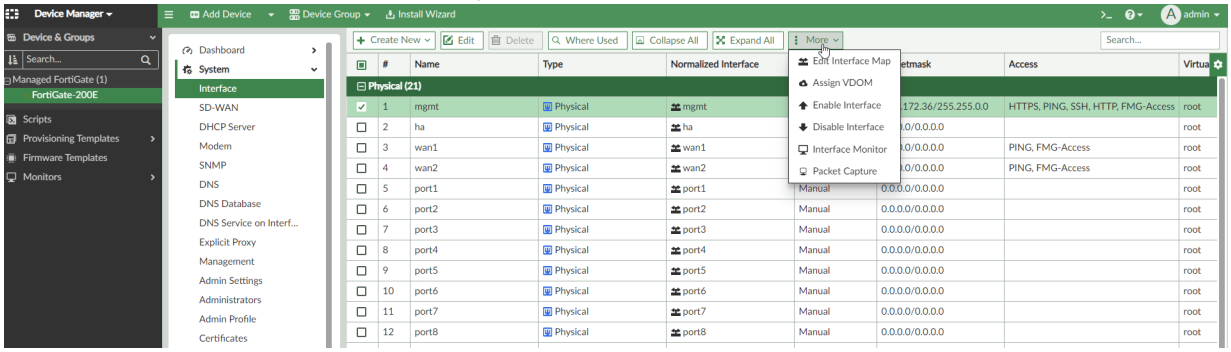
## Perform packet capture on managed FortiGate interfaces and on managed FortiSwitches - 7.2.2

FortiManager can perform packet capture on managed FortiGate interfaces and trigger packet capture on the managed FortiSwitches when traffic-sniffer has been configured. The captured file can be saved and downloaded as .pcap file for further analysis.

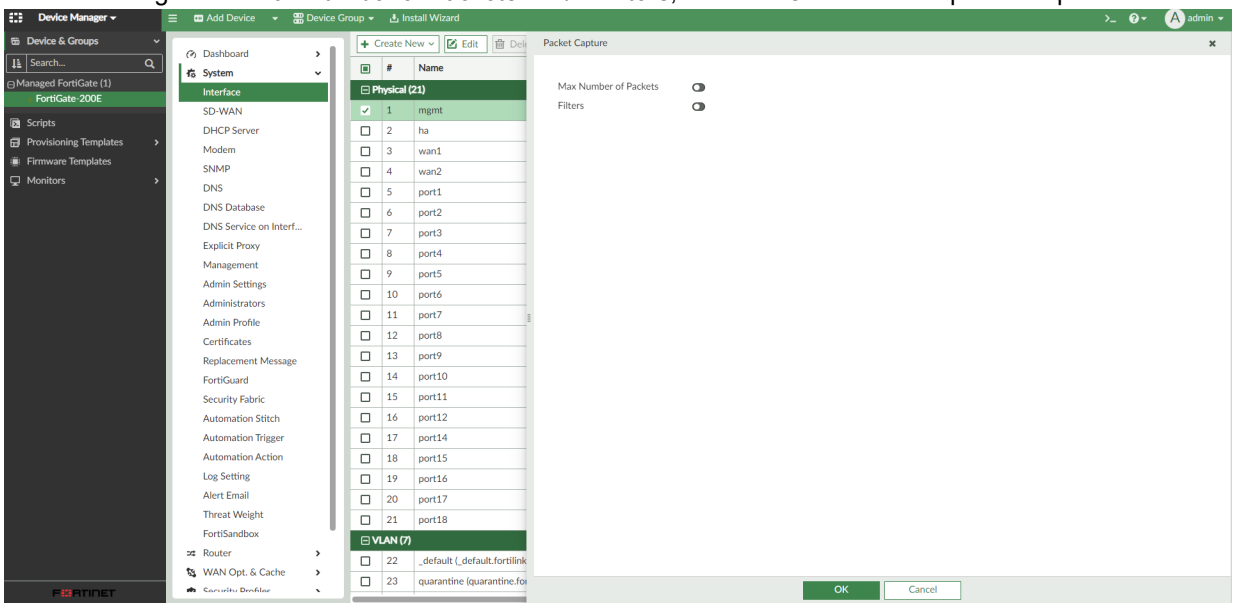
### Packet Capture in the Device manager

**To perform a packet capture on managed FortiGate interfaces:**

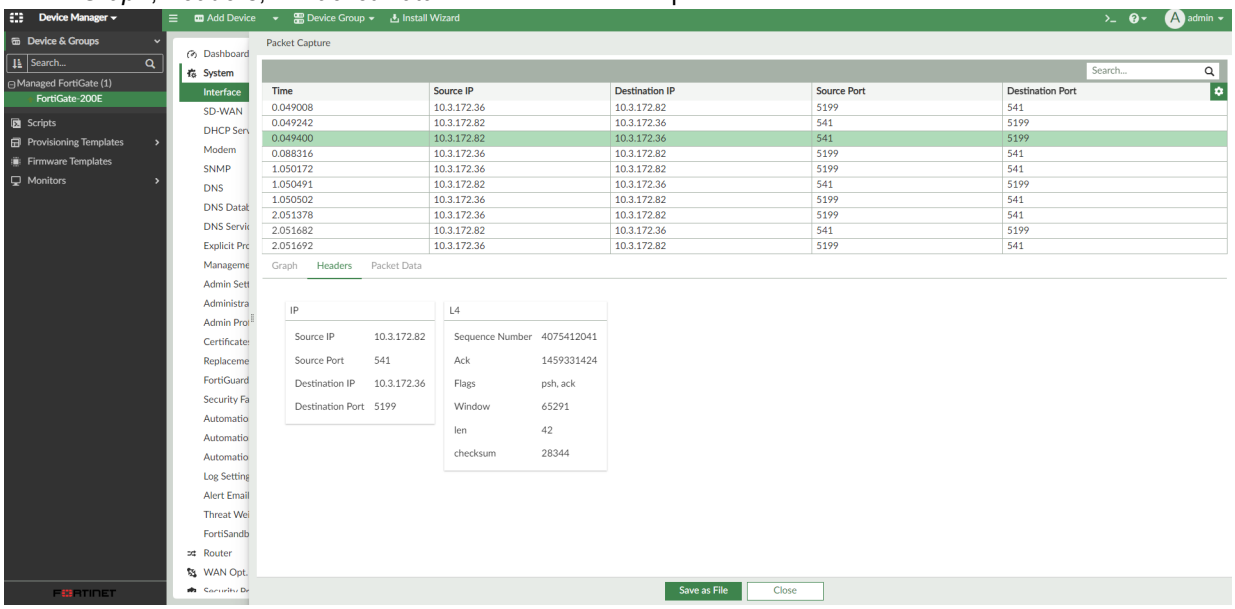
1. In *Device Manager*, select a FortiGate and go to *System* > *Interface*.
2. Select an interface, click *More* > *Packet Capture*.



3. You can configure the *Max Number of Packets* and/or *Filters*, and click *OK* to start the packet capture.




4. Select *Graph*, *Headers*, or *Packet Data* to view details of the packet.




## Packet Capture in the FortiSwitch Manager

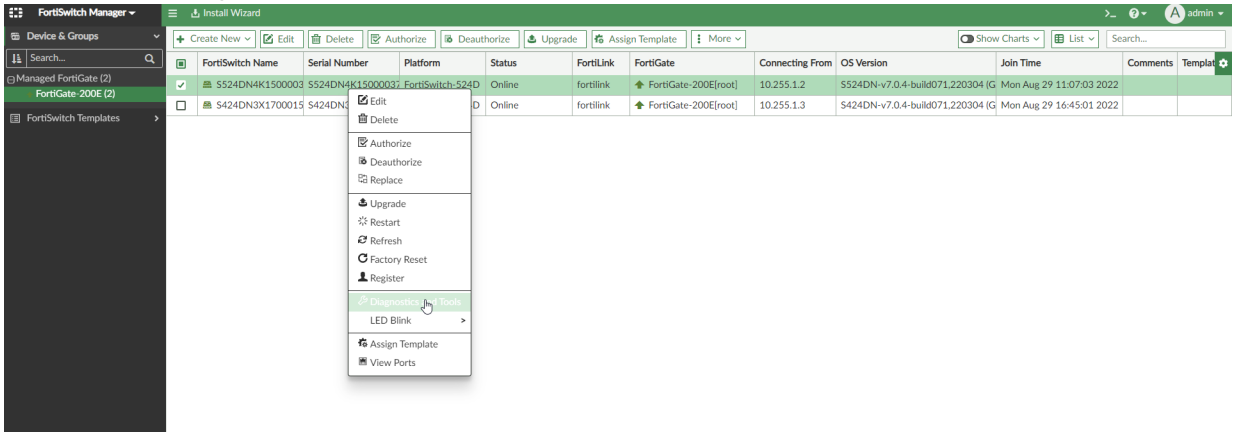
**To perform a packet capture on managed FortiSwitch devices:**

1. In the FortiGate CLI, configure the `switch-controller traffic-sniffer` setting.
   For example:

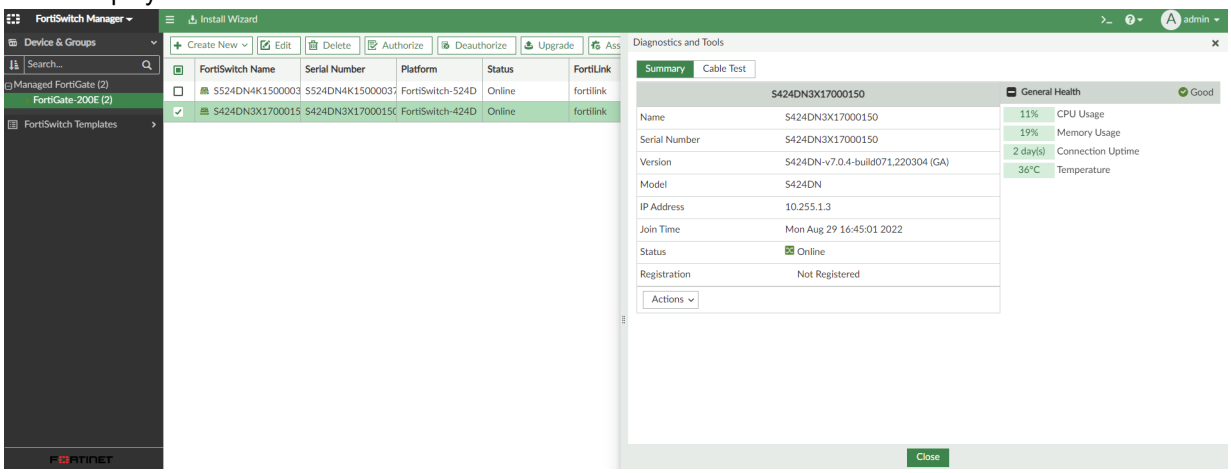
```
config switch-controller traffic-sniffer
   set mode rspan
   config target-mac
      edit 00:0c:29:1a:2b:3c
         set description "ABC123"
      next
```

```
end
config target-ip
   edit 192.168.11.11
      set description "ABC123IP"
   next
end
config target-port
   edit "S000DN4K15000050"
      set description "ABC123switch"
      set out-ports "port1"
   next
end
```

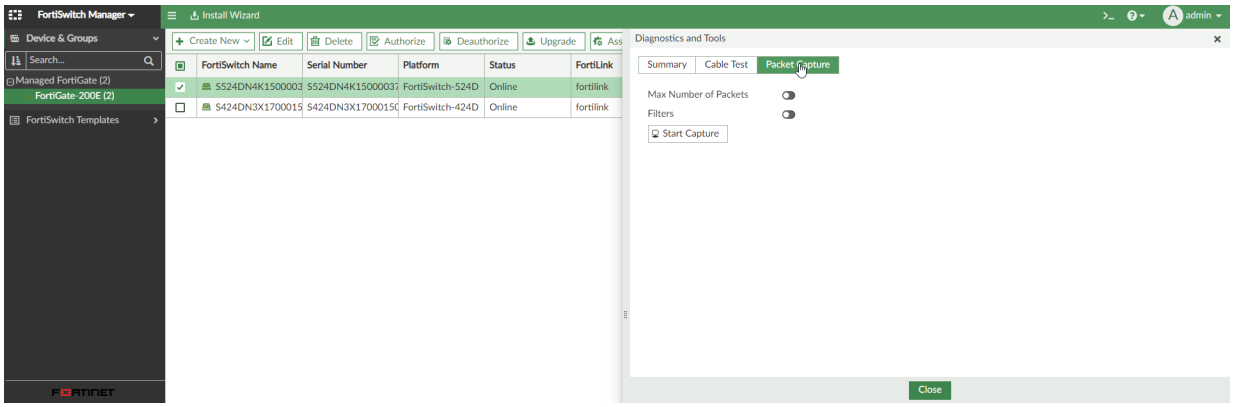
2. After the FortiGate has been added in FortiManager, go to *FortiSwitch Manager*, select a FortiSwitch device, right-click and select *Diagnostics and Tools*.



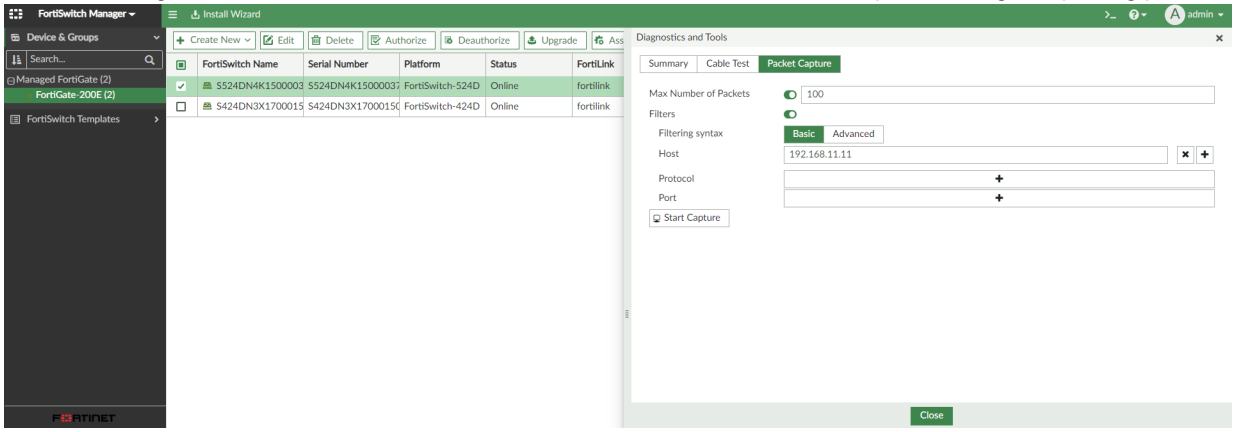

3. When the FortiSwitch is not configured in `switch-controller traffic-sniffer`, the *Packet Capture* tab will not be displayed.



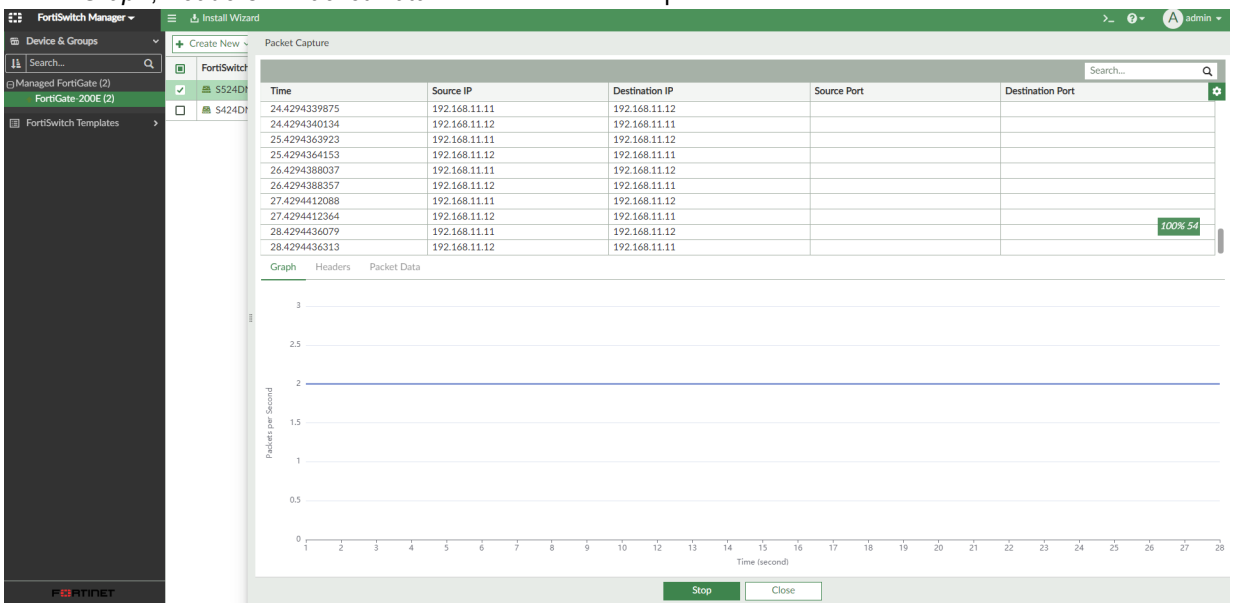
4. When the FortiSwitch is configured in `switch-controller traffic-sniffer`, the *Packet Capture* tab is shown.

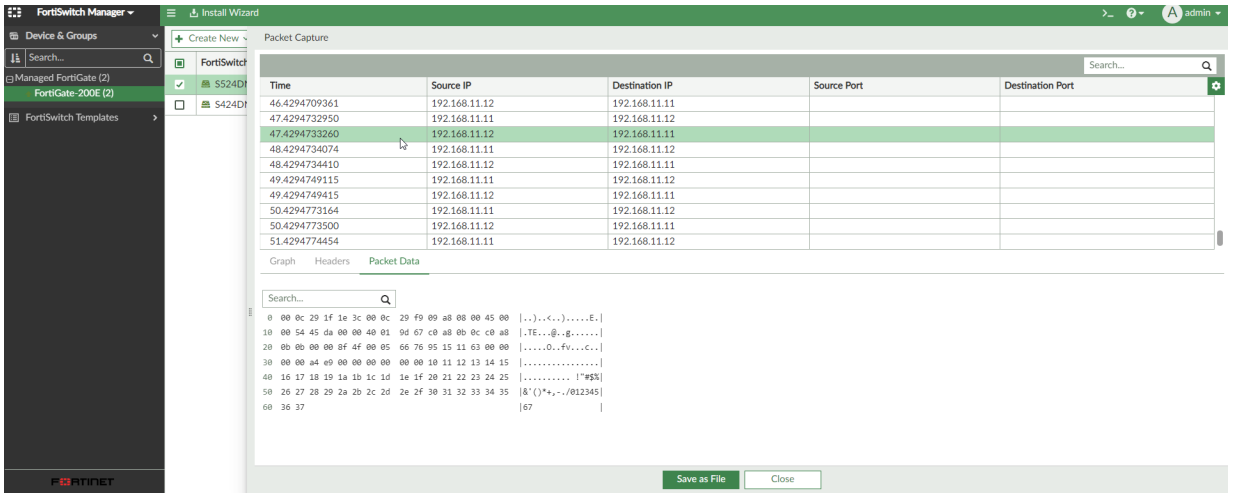



5. You can configure the *Max Number of Packets* and/or *Filters*, and click *Start Capture* to begin capturing packets.

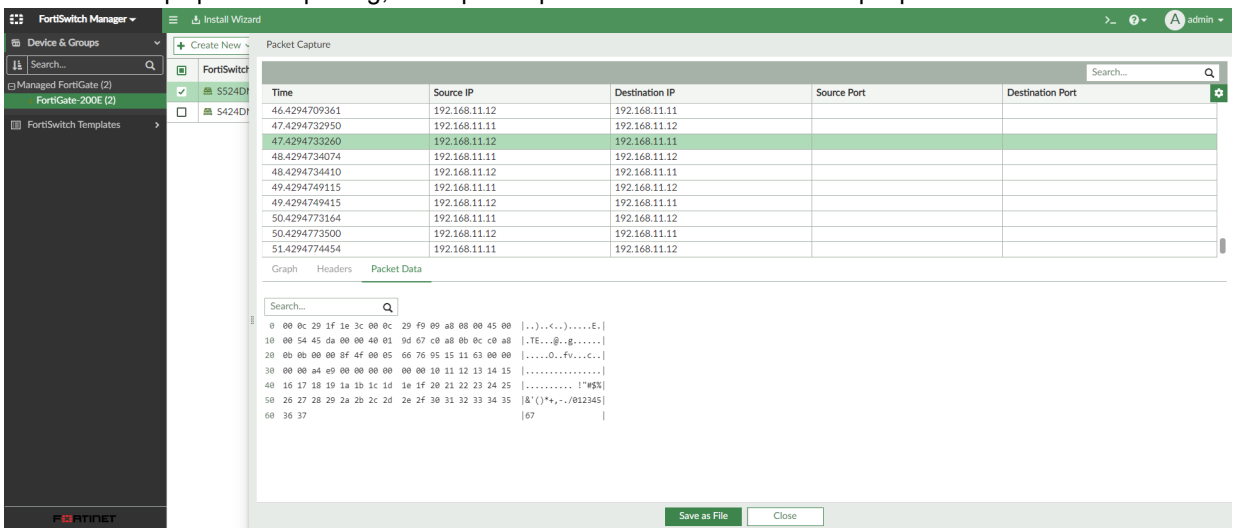


6. Select *Graph*, *Headers* or *Packet Data* to view details of the packet.




7. When user stops packet capturing, the captured packets can be saved into a .pcap file.



## FortiManager supports FortiGate Cloud-Native Firewall as device type - 7.2.2

Fortimanager can be used to install and monitor security features on FortiGate Cloud-Native Firewall (CNF) instances that are deployed on AWS.

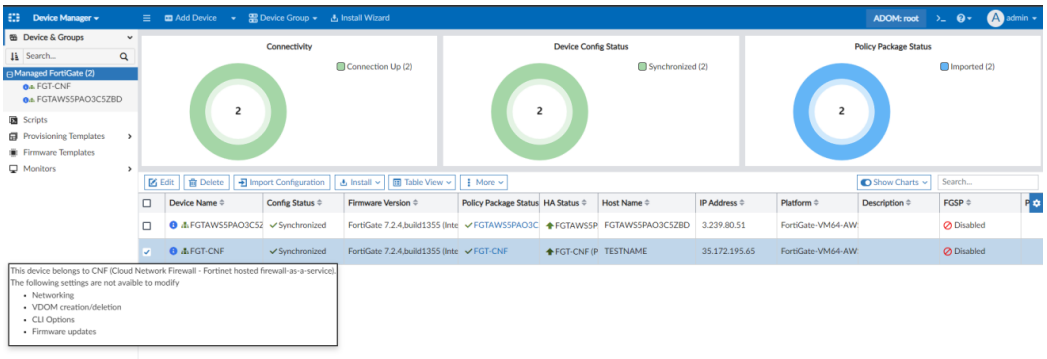
FortiGate CNF is software-as-a-service that simplifies cloud network security while providing availability and scalability. FortiGate CNF reduces the network security operations workload by eliminating the need to configure, provision, and maintain any firewall software infrastructure while allowing security teams to focus on security policy management. FortiGate CNF offers you the flexibility to procure on demand or use annual contracts.

**To manage FortiGate CNF from FortiManager:**

1. In FortiGate CNF, in the *Display Primary FortiGate Information* field in the *Edit CNF* form, find the FortiGate connection details.
2. In FortiManager, go to *Device & Groups* > *Add Device*.
3. Click *Discover Device*.
4. Enter the *IP Address* of the FortiGate CNF instance.
5. Enable *Use Legacy Device Login* and enter the *User Name* and *Password*, then click *Next*.
6. Update or enter any required details and click *Next*.
7. Click *Finish*. The FortiGate CNF instance is added to FortiManager. There may be a short delay before the device is available.

---

FortiGate CNF clusters are treated differently than the normal FortiGate auto-scale cluster on AWS. Hover over the information icon next to the cluster name to see more information about the cluster.



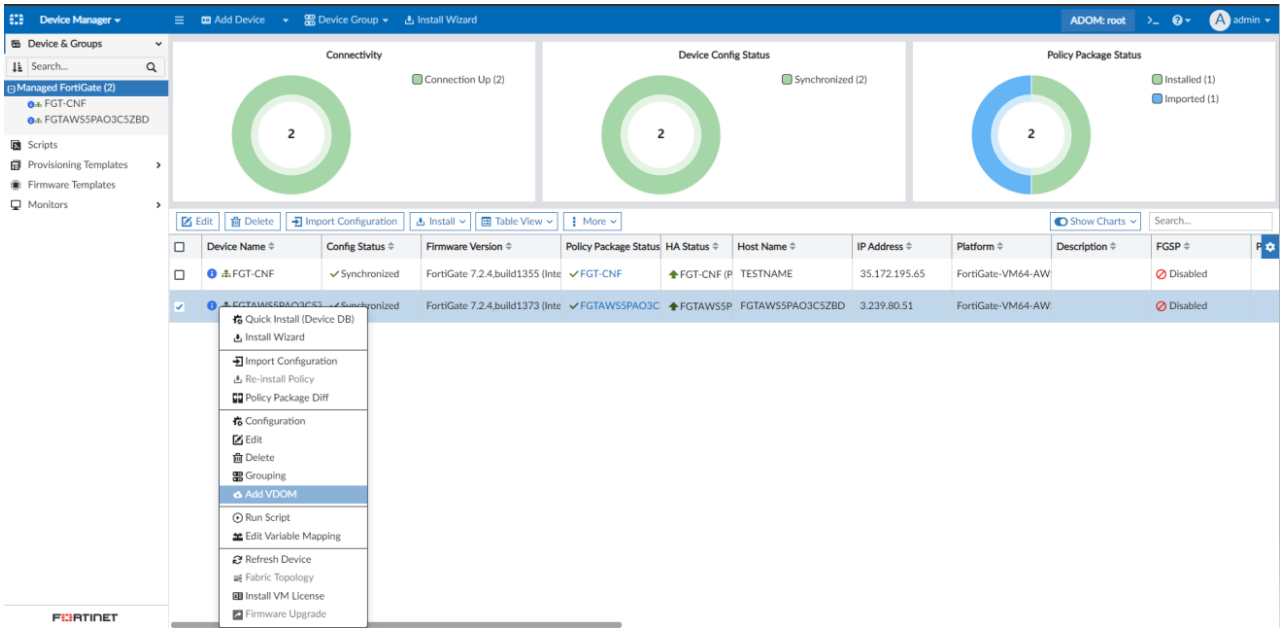

---

## Management restrictions

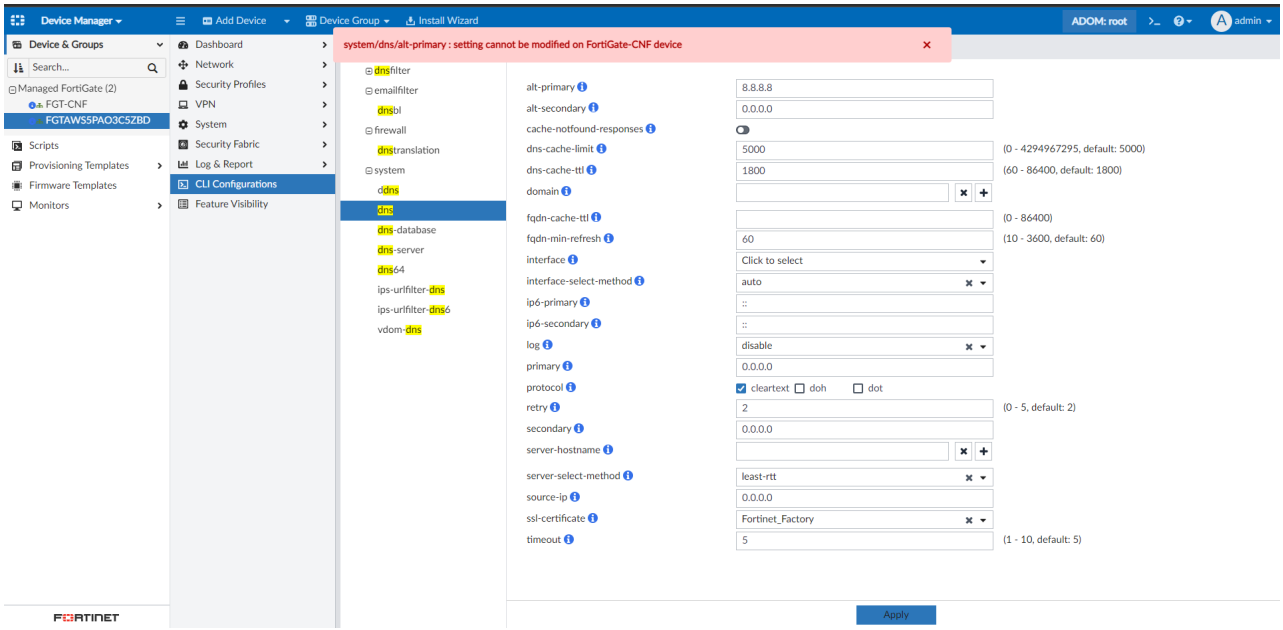
Fortigate CNF is Fortinet-managed service and there are limited configurations that are permitted from FortiManager.

The following management operations are restricted:

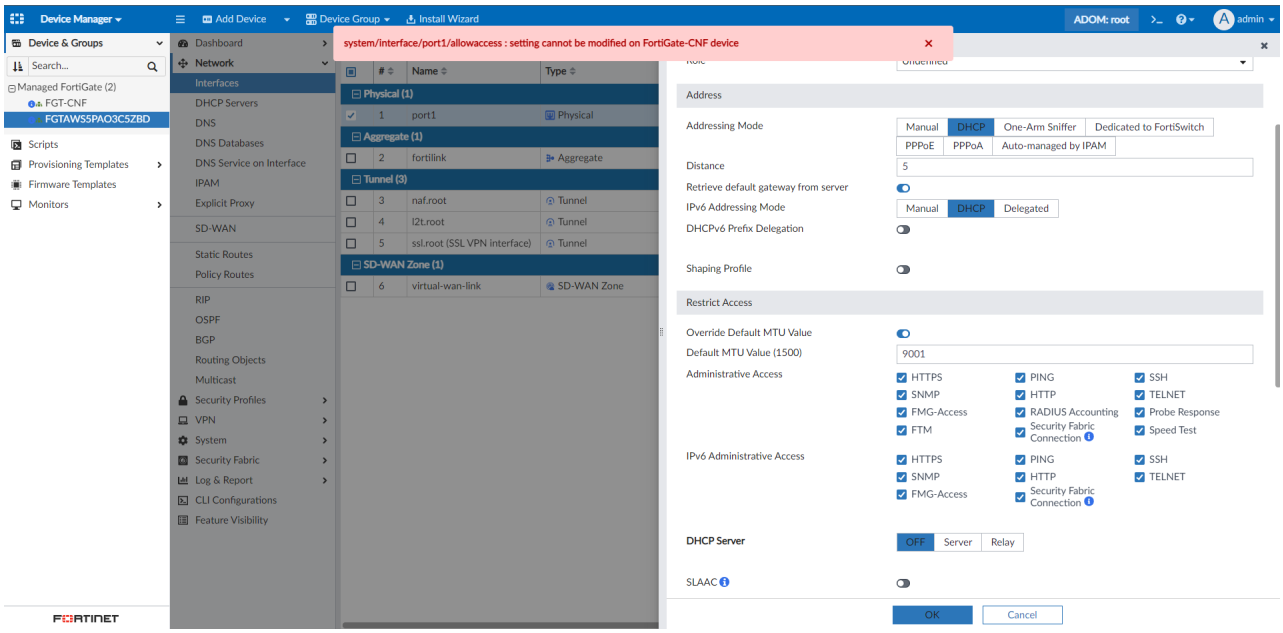
- VDOM creation is not permitted and the option is greyed out.



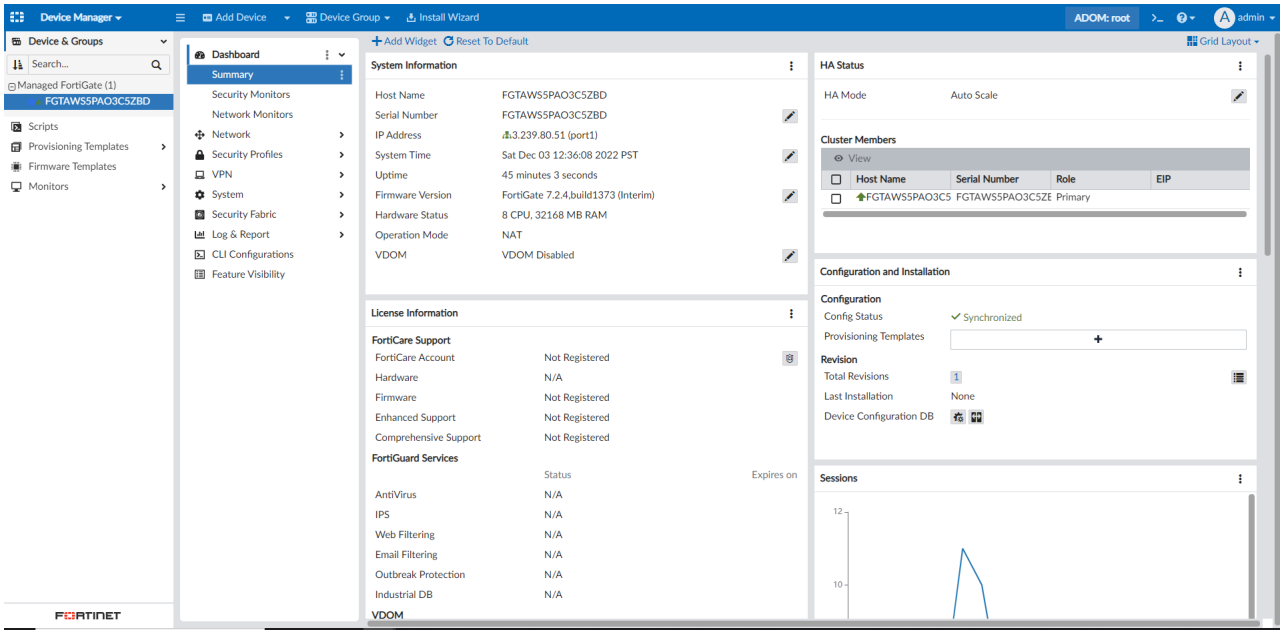

- Changes in CLI configuration are not permitted and if tried there is an error.




- Changes to networking components of the FortiGate are restricted and if tried there is an error.




- CLI access to the FortiGate CNF instance is not allowed from FortiManager.

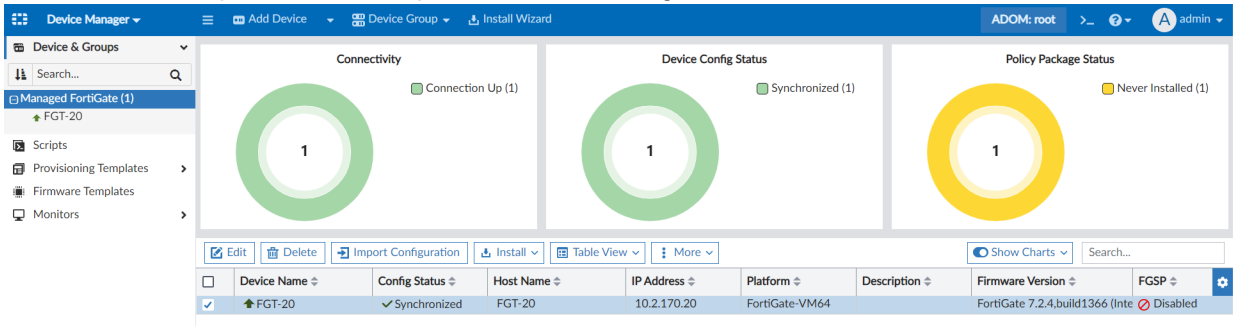



## Interface-based traffic shaping can display real time dropped packets - 7.2.2

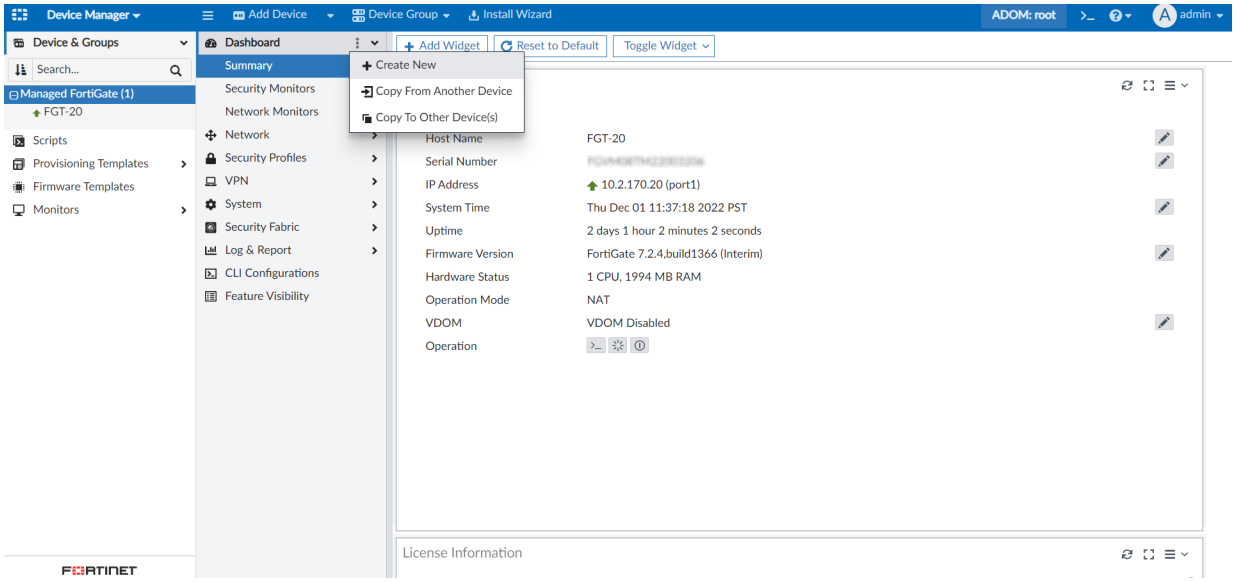
Interface-based traffic shaping can display real time dropped packets.

**To view real-time dropped packets in the Traffic Shaping widget:**

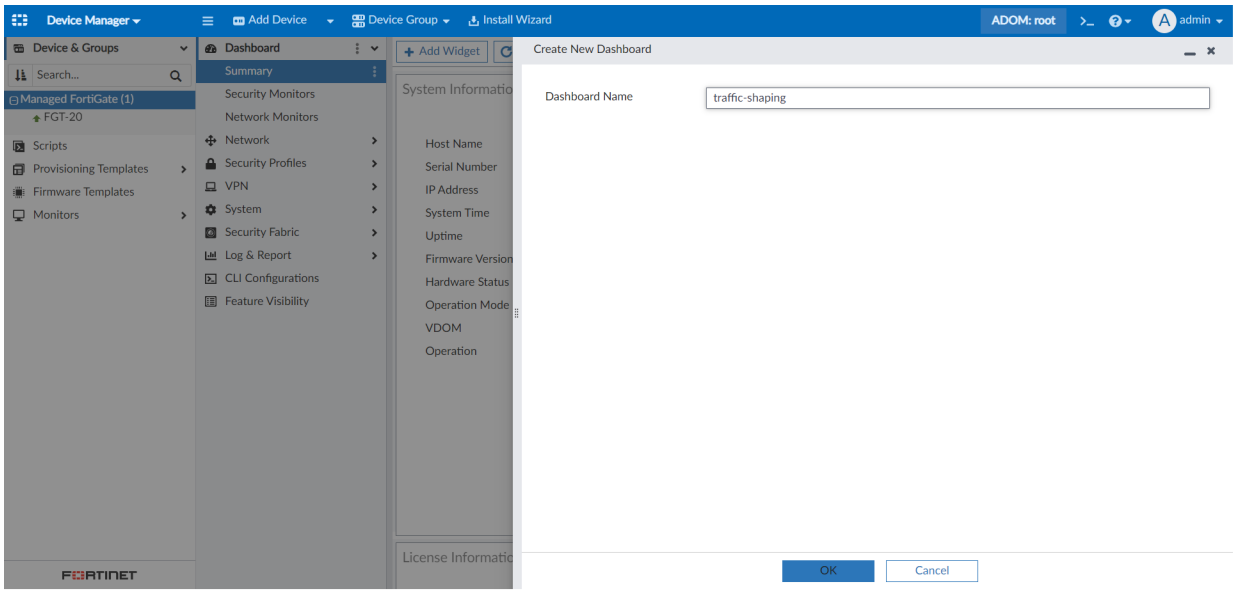
1. Go to *Device Manager* > *Device Groups*, and select a managed device.



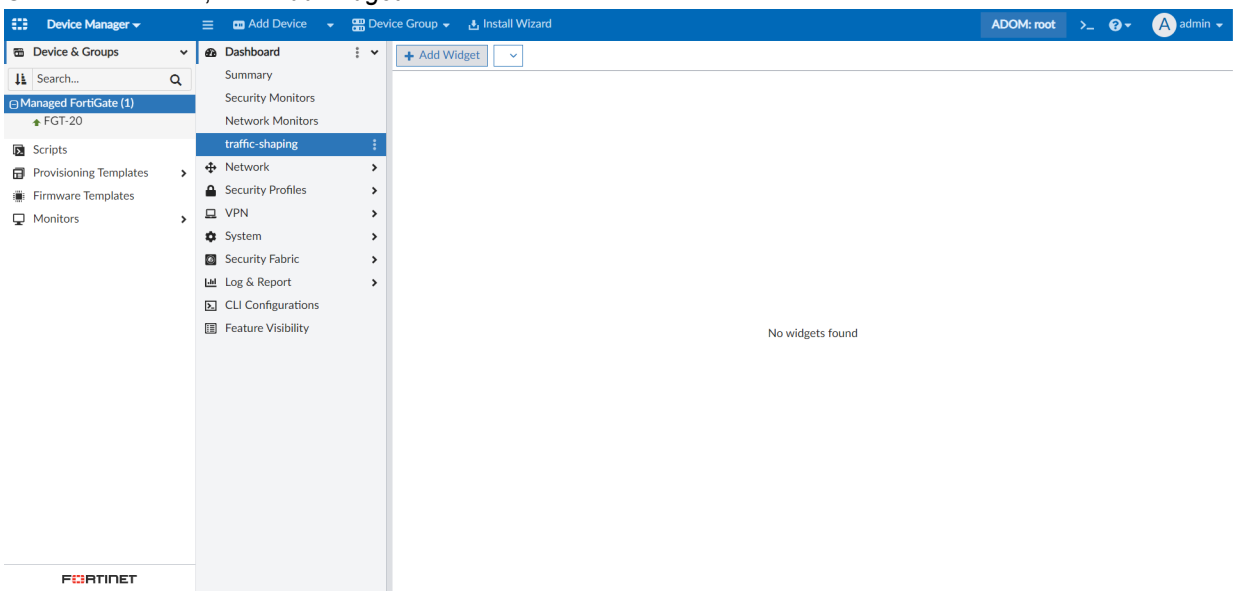

2. In the toolbar, click *Create New*.



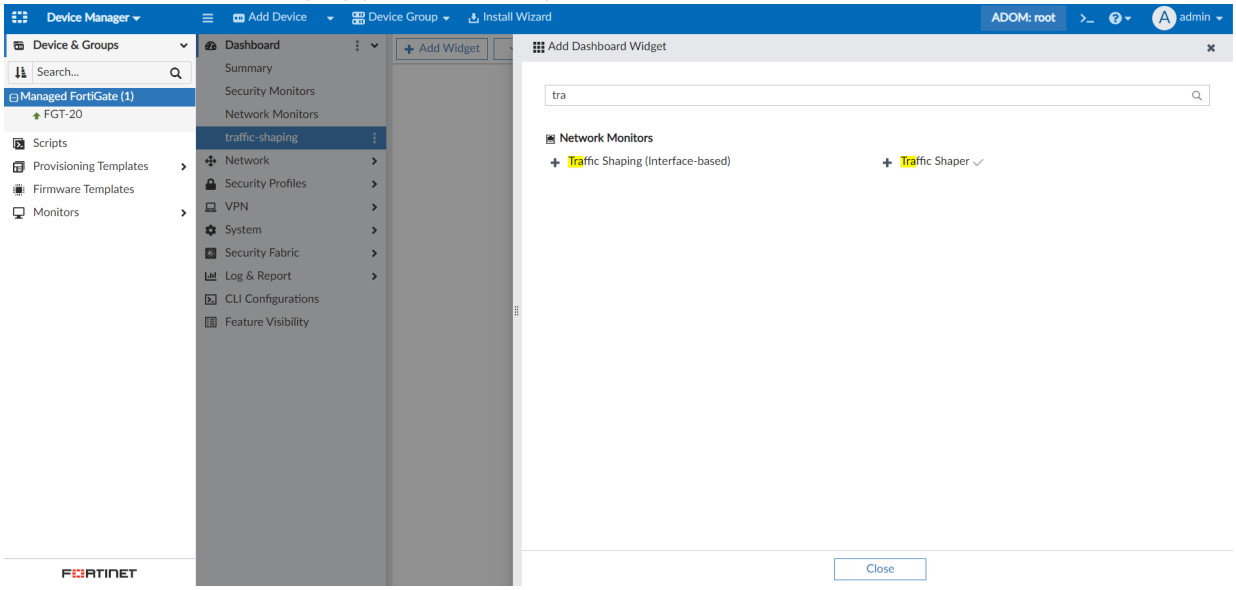

3. Enter a name for the dashboard.



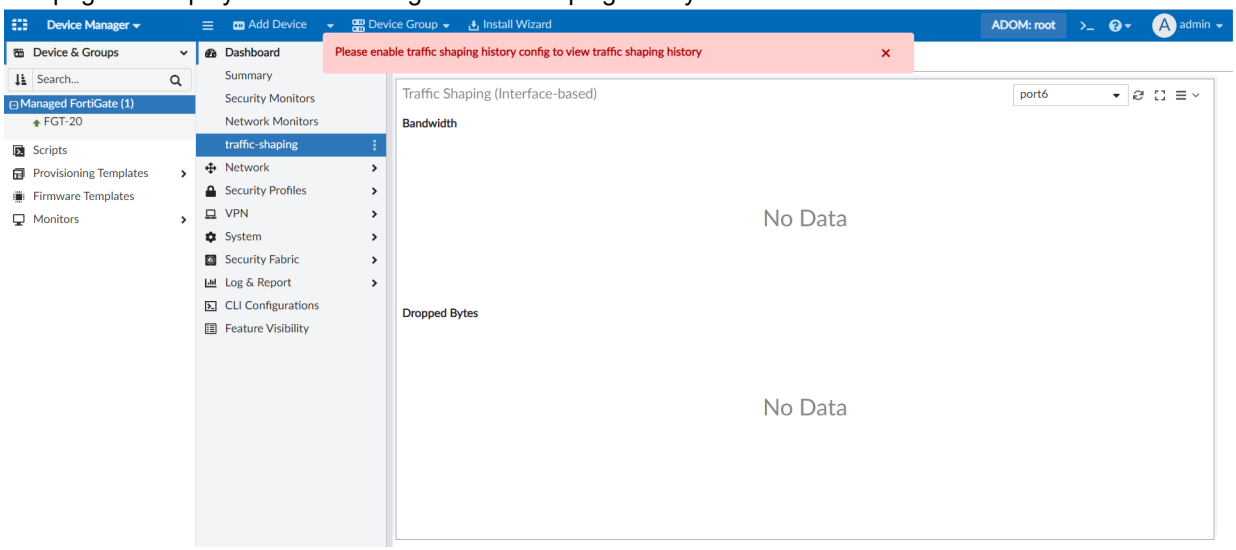
4. On the dashboard, click *Add Widget*.




5. Search and add *Traffic Shaping (Interface-Based)*.



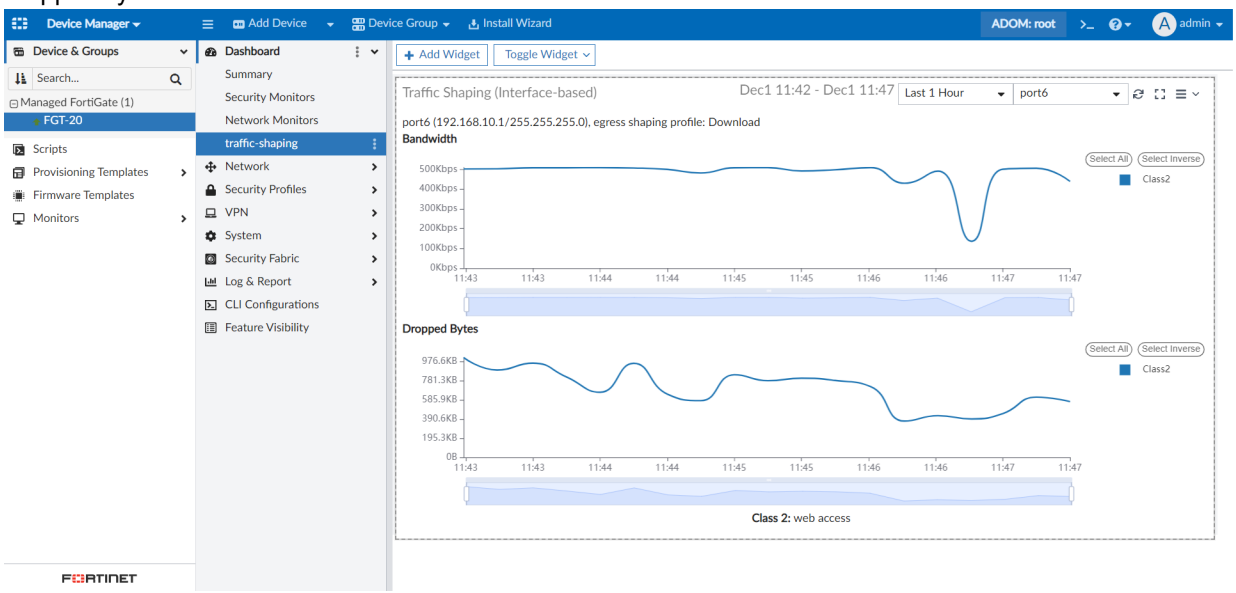
The page will display an error message if traffic shaping history is not enabled.




6. To enable traffic shaping history, open the CLI console and enter the following commands:

```
config system admin setting
   set traffic-shaping-history enable
end
```

7. After FortiManager receives data from FortiGate, the widget will display the real-time information of bandwidth and dropped bytes for each class.

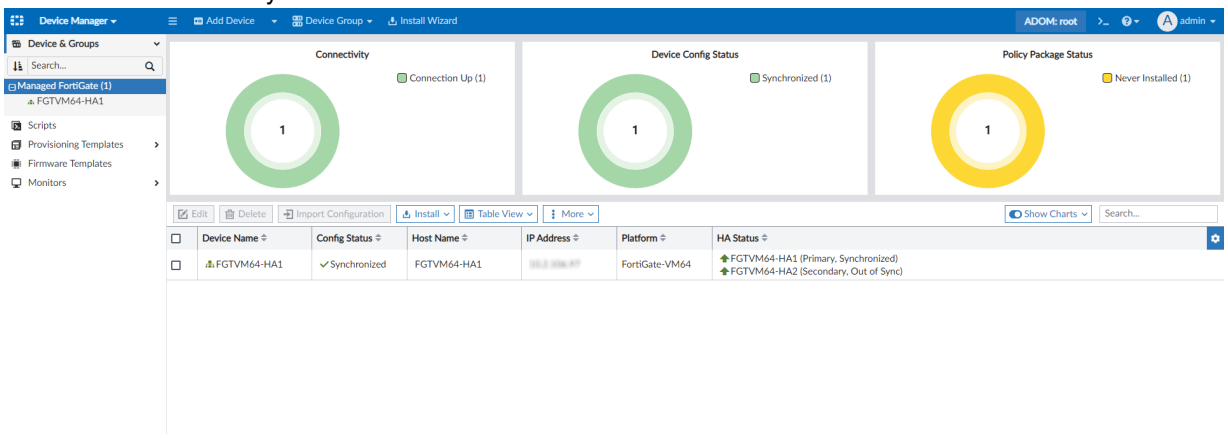



## FortiManager detects and displays the out-of-sync status of the FortiGate HA Cluster nodes - 7.2.2

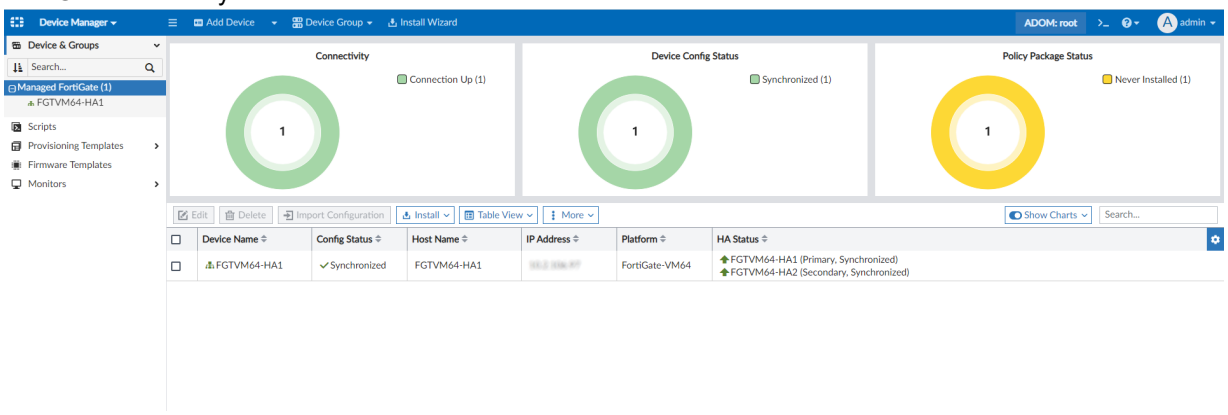
FortiManager detects and displays the out-of-sync status of the FortiGate HA Cluster nodes.

**To view the out-of-sync status of FortiGate HA cluster nodes on FortiManager:**

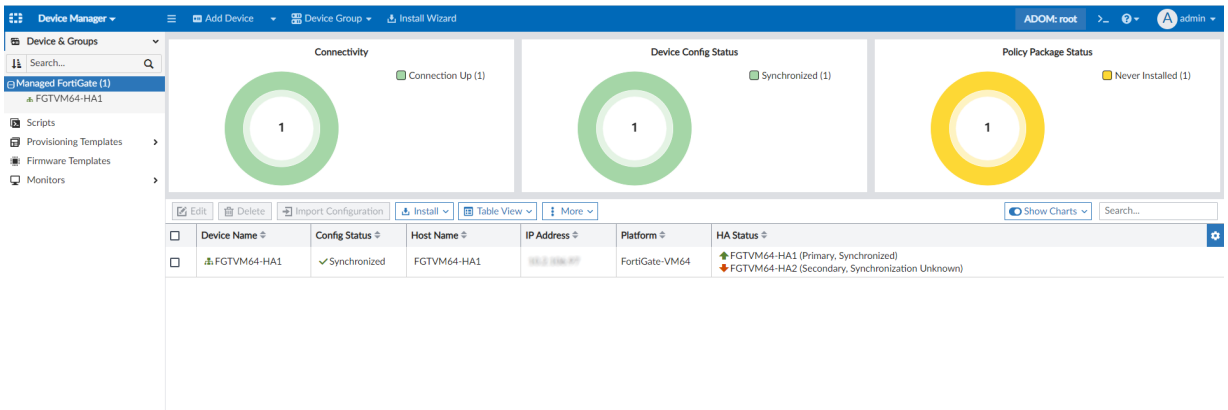
1. Go to the *Device Manager*, and click *Managed FortiGate*.
   FortiManager displays the following information about the status of FortiGate HA clusters:
   - FortiGate HA is out-of-sync.




   - FortiGate HA is in sync.

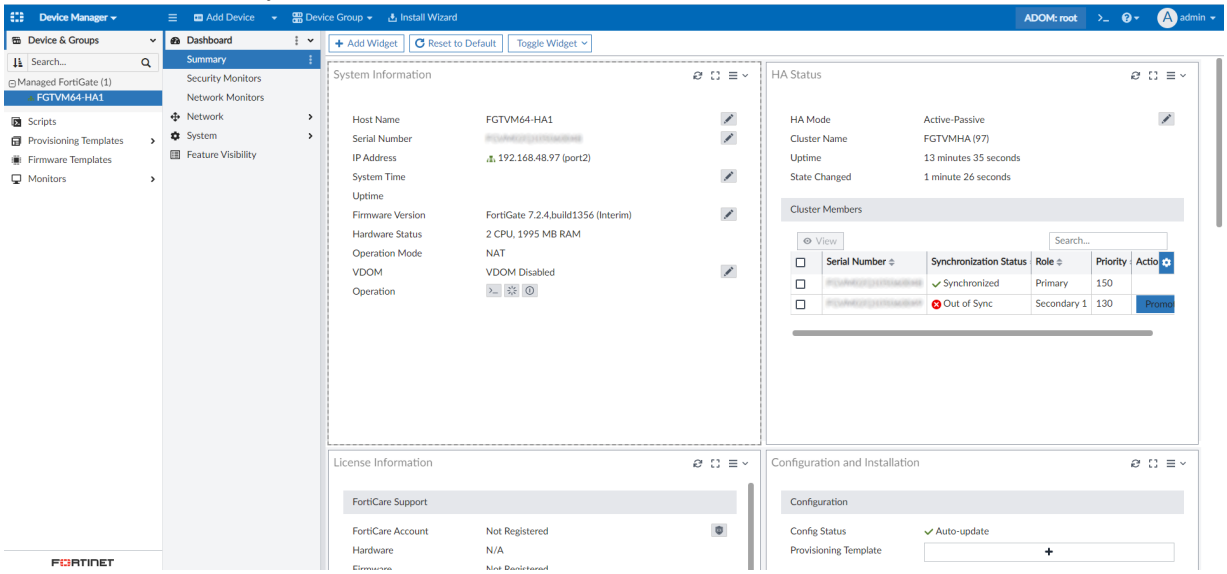



   - A FortiGate cluster members is offline.

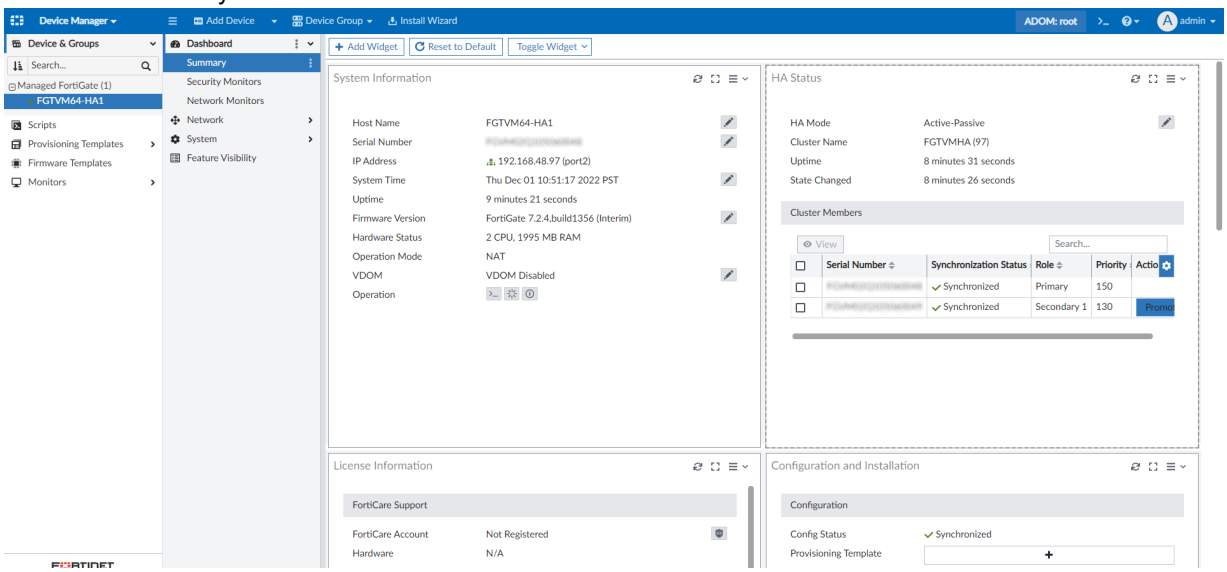



2. Select an HA member device in the Device Manager to view the device database.
   FortiManager displays the following information about the status of FortiGate HA clusters:

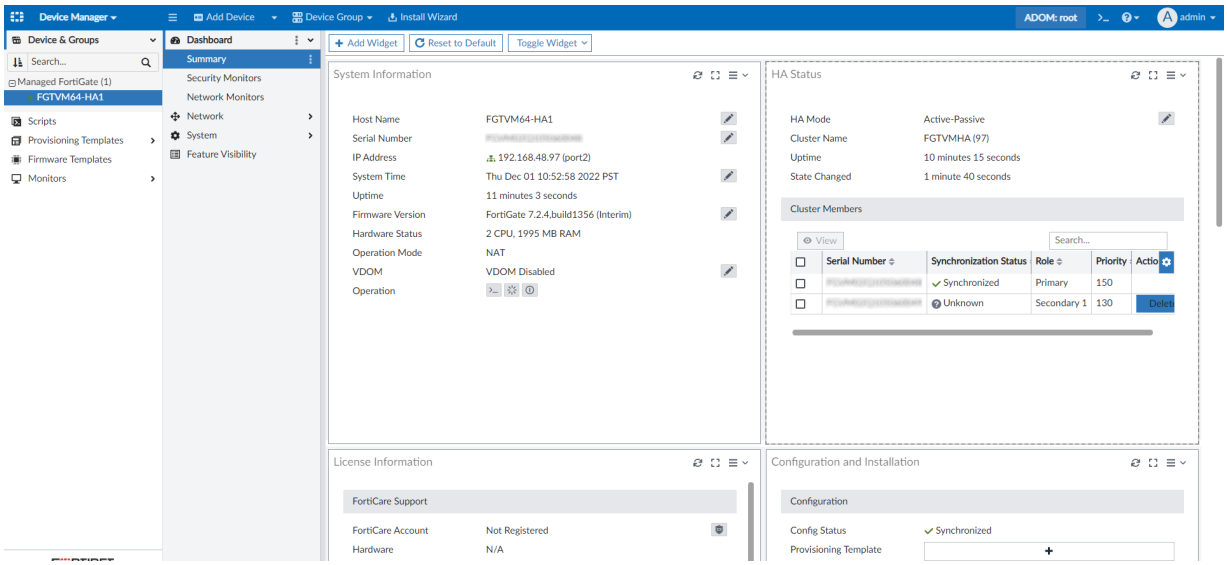
- FortiGate HA is out-of-sync.




- FortiGate HA is in sync.



- A FortiGate cluster members is offline.




# SD-WAN

This section lists the new features added to FortiManager for SD-WAN:

- SD-WAN overlay templates on page 39
- SD-WAN Monitor includes new filter to display unhealthy devices or interfaces only 7.2.1 on page 45
- Pre-built route-maps used for SD-WAN self-healing with BGP routing 7.2.2 on page 47
- SD-WAN Template added the health-check embedded SLA information 7.2.2 on page 49
- FortiManager supports multiple interface members in the SD-WAN neighbor configurations 7.2.2 on page 52

## SD-WAN overlay templates

Most SD-WAN deployments require complex overlay configurations for datacenter or cloud connectivity. FortiManager 7.2.0 includes an SD-WAN overlay template with a wizard to automate and simplify the process using Fortinet's recommended IPsec and BGP templates.

Note that the overlay template does not provide any SD-WAN intelligence. Please configure a SD-WAN template to complete the SD-WAN configuration. The overlay template also assumes connectivity between the HUB and branch in order to build the overlay tunnels. This can be accomplished in a variety of ways, such as static routes, dynamic routing protocol (BGP) or through a DHCP provided static route.

This topic includes the following.

- Prerequisites and network planning on page 40
- Using the SD-WAN overlay template on page 40
- Configuring an SD-WAN overlay template on page 40

For more information, including editing a template and onboarding new SD-WAN branch devices, see the FortiManager Administration Guide.

## Prerequisites and network planning

### Prerequisites

- Import the FortiGate devices that will make up the hub and branch devices into FortiManager.
- Configure the ISP links and other interfaces on your imported devices.
- Create a device group for your branch devices.

### Network planning

- Allocate the overlay network address space. By default, the template uses `10.10.0.0/16`.
- Allocate the loopback IP address space. By default, the template uses `172.16.0.0/16`.
- Select an AS number for BGP for the new SD-WAN overlay region. By default, the template uses `65000`.

## Using the SD-WAN overlay template

**To use the SD-WAN overlay template:**

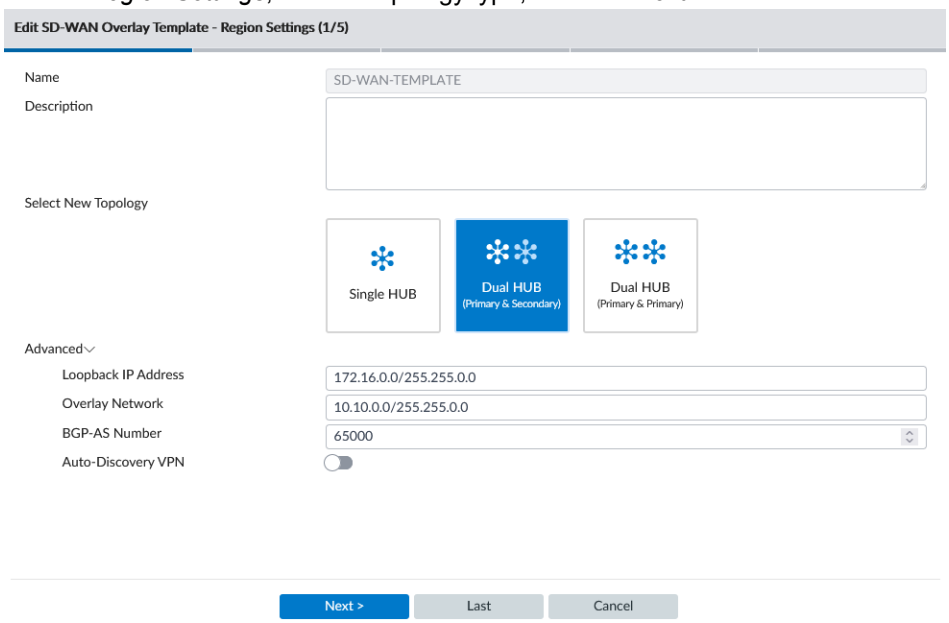
1. Pre-configure your network and SD-WAN devices.
2. Create an SD-WAN overlay template.
3. Assign metadata variables to devices. The branch_id variable is automatically created by the template and each branch device must be assigned a unique value. Additional custom metadata variables can be used if required.
4. Configure the SD-WAN rules to include the newly created overlays by creating or editing an SD-WAN template.
5. Create the Policy Package for your branch and hub devices.
6. Install the changes to SD-WAN devices using the Install Wizard.
7. (Optional) Edit the SD-WAN overlay template.
8. (Optional) Add new branch devices.

## Configuring an SD-WAN overlay template

**To create an SD-WAN overlay template:**

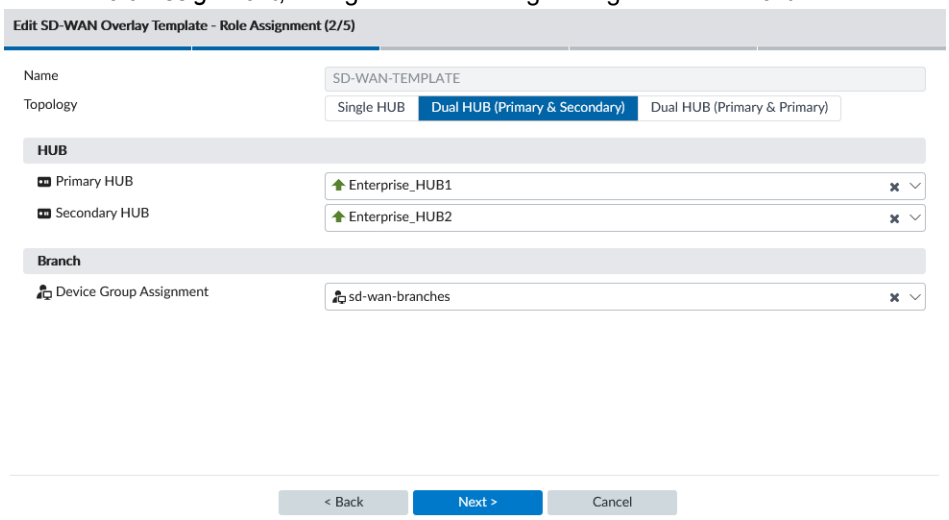
1. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Overlay Templates*.
2. Click *Create New*.
   The Create New SD-WAN Overlay Template wizard opens.
3. Enter a name and description for the new SD-WAN overlay template, and click *OK*.

4. For the *Region Settings*, select a topology type, and click *Next*.



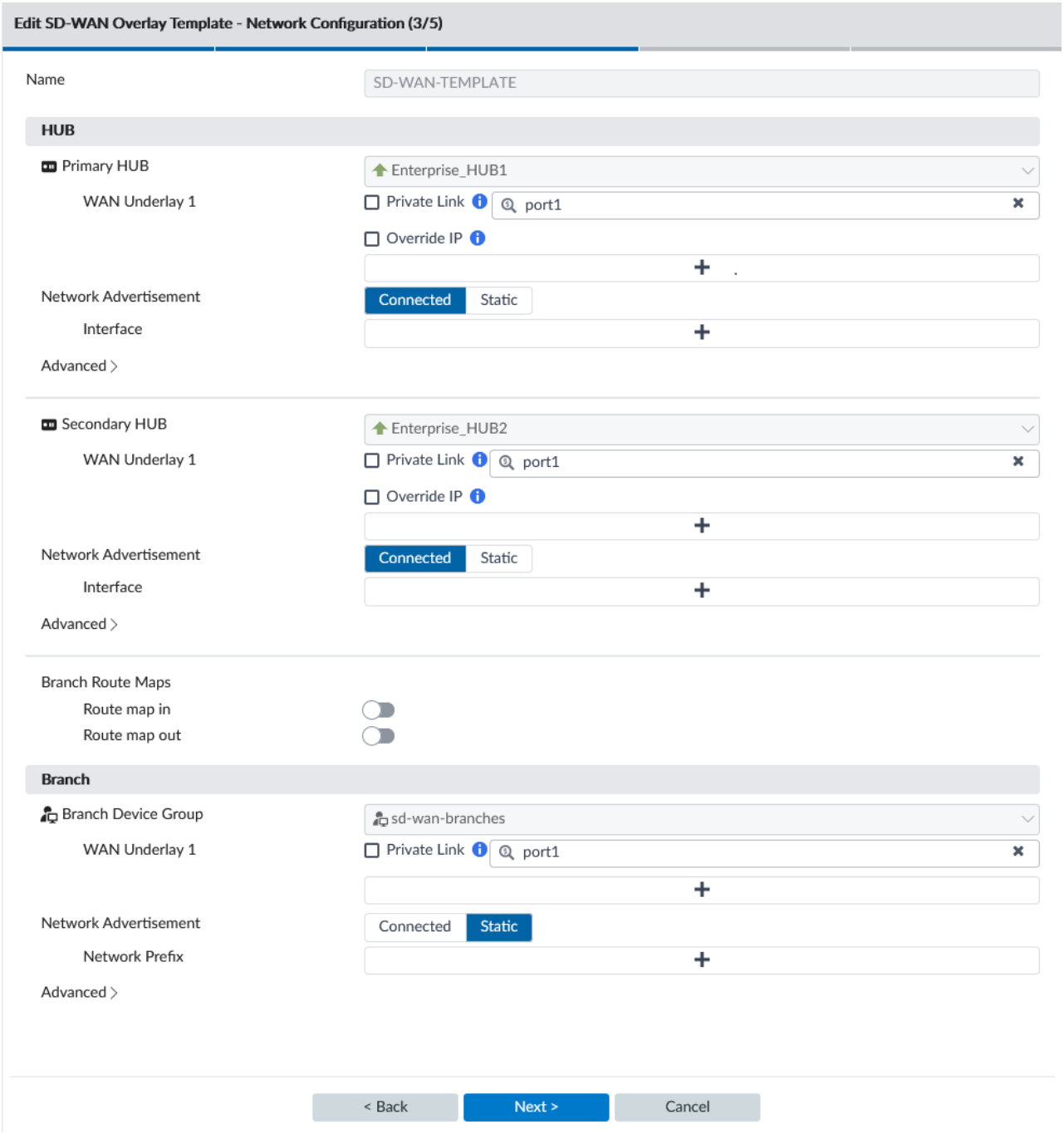

| | | |
|---|---|---|
| **Select New Topology** | | Select a topology type based on your environment. Topologies include the following:<br>• Single Hub<br>• Dual Hub (Primary/Secondary)<br>• Dual Hub (Primary/Primary)<br>The options presented in the wizard change based on the topology selected.<br><br>Primary/Secondary and Primary/Primary are the same configuration, with the difference being that in a Primary/Secondary deployment, the Secondary hub is given a higher cost than the Primary. This cost is controlled by the SDWAN rule. |
| **Advanced** | | Expand to view additional configurable settings.<br>These fields are preconfigured with settings that will work in many situations, but you may need to adjust these to match your own networking environment. They should match the addresses you identified when considering the SD-WAN overlay template prerequisites. |
| | **Loopback IP Address** | Optionally, you can configure the loopback IP address.<br>By default, this setting is set to `172.16.0.0/255.255.0.0`. |
| | **Overlay Network** | Optionally, you can configure the overlay network.<br>By default, this setting is set to `10.10.0.0/255.255.0.0`. |
| | **BGP-AS Number** | Optionally, you can configure the BGP AS number.<br>By default, this setting is set to `65000`. |
| | **Auto-Discovery VPN** | Optionally, you can toggle this setting ON to enable Auto Discovery VPN (ADVPN). |

5. For the *Role Assignment*, configure the following settings and click *Next*.




| | |
|---|---|
| **Topology** | Optionally, you can change the topology type that you selected on the previous screen. |
| **Hub** | Select the SD-WAN hubs. The number of hubs required depend on the topology selected:<br>• *Single Hub*: One standalone hub.<br>• *Dual Hub (Primary & Secondary)*: One primary and one secondary hub.<br>• *Dual Hub (Primary & Primary)*: Two primary hubs.<br>Hub devices must be added to FortiManager before creating the SD-WAN overlay template. |
| **Branch** | Select the device group containing your SD-WAN branch devices.<br>Devices included in this device group are configured as SD-WAN branch devices as a part of this template.<br>Additional devices can be added to the selected device group later to receive the SD-WAN branch configuration when performing an installation on that device. This simplifies the onboarding of new branch devices. |

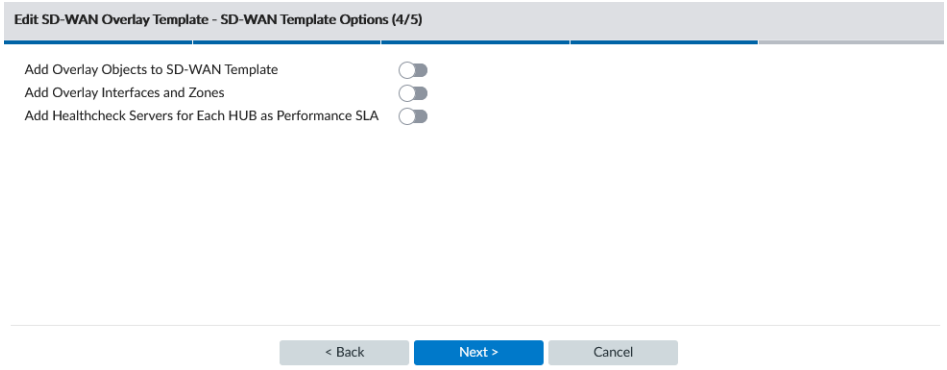
6. For the *Network Configuration*, configure the following settings and click *Next*.




| | |
|---|---|
| **Hub** | Configure the network settings for each hub in your configuration. The number and types of hubs present depend on the topology you selected. |
| **WAN Underlay** | Type the interfaces for each WAN underlay. You can add additional WAN underlays by clicking the add icon.<br>For each WAN underlay, you can optionally enable the following settings:<br>• *Private Link*: No overlays will be created on private links. |

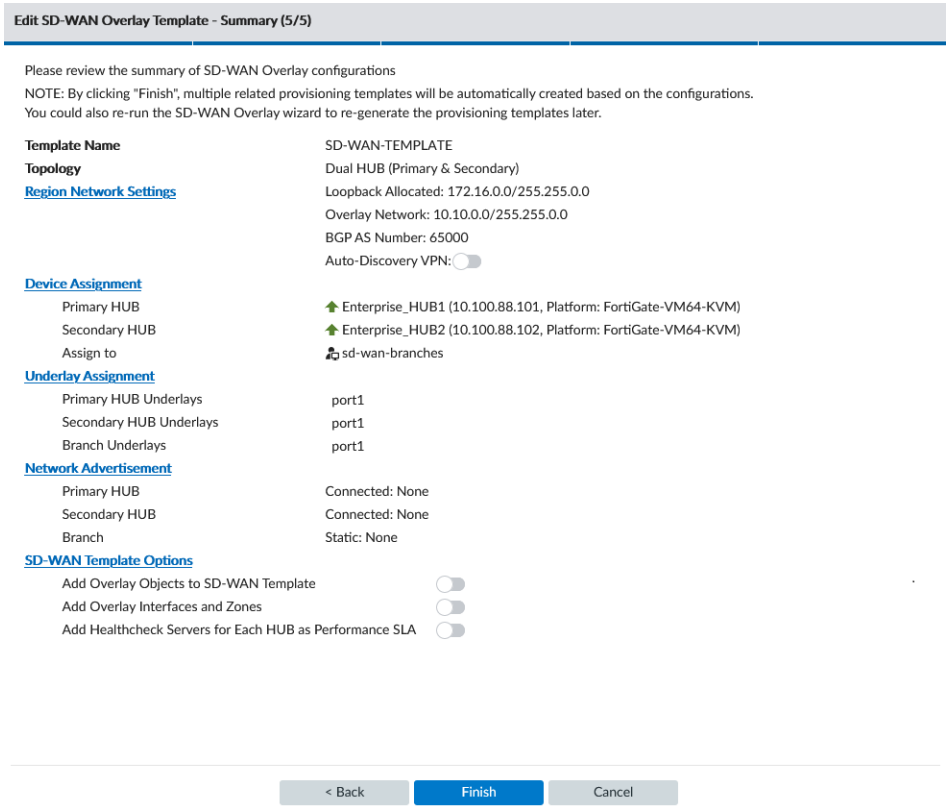
| | | |
|---|---|---|
| | | • *Override IP*: Override the IP address for the WAN underlay with the provided IP address. This option is not available when *Private Link* is enabled. |
| | **Network Advertisement** | 1. Configure network advertisement for the hub. Network advertisement can be set to one of the following:<br>• *Connected*: Type the network interface to advertise. Additional interfaces can be added by clicking the add icon.<br>• *Static*: Type the network prefix to advertise. Additional network prefixes can be added by clicking the add icon. |
| | **Advanced** | Expand to view advanced settings, including configuration of SD-WAN neighbors.<br>Click *Neighbors* > *Create New* to add a new SD-WAN neighbor for the hub. |
| **Branch Route Maps** | | Optionally, move the toggle to the ON position to enable branch maps, and then select the corresponding route map. You can create a new route map by clicking the add icon. |
| **Branch** | | Configure the network settings for the branch devices in your configuration. |
| | **WAN Underlay** | Type the interfaces for the SD-WAN branch WAN underlay. You can add additional WAN underlays by clicking the add icon.<br>For each WAN underlay, you can optionally enable the following settings:<br>• *Private Link*: No overlays will be created on private links. |
| | **Network Advertisement** | Configure network advertisement for the branch. Network advertisement can be set to one of the following:<br>• *Connected*: Type the network interface to advertise. Additional interfaces can be added by clicking the add icon.<br>• *Static*: Type the network prefix to advertise. Additional network prefixes can be added by clicking the add icon. |
| | **Advanced** | Expand to view advanced settings, including configuration of route maps for hub overlays. You can apply the route map settings to all hub overlays or specify them individually. |

7. For the *Template Options*, configure the following settings and click *Next*.



| | |
|---|---|
| **Add Overlay Objects to SD-WAN Template** | Optionally, you can toggle this setting ON to automatically add the overlay objects configured by this template to a new or existing SD-WAN template.<br>Select an existing SD-WAN template or click the add icon to create a new SD-WAN template. |
| **Add Overlay Interfaces and Zones** | Optionally, you can toggle this setting ON to add overlay interfaces and zones. |
| **Add Healthcheck Servers for Each HUB as Performance SLA** | Optionally, you can toggle this setting ON to add health check servers for each hub as performance SLAs. |

8. The summary window displays a summary of the SD-WAN overlay configurations that will be created by this template.
9. When you click *Finish*, multiple provisioning templates are created based on the information you provided. The templates are automatically assigned to the devices specified by the wizard.



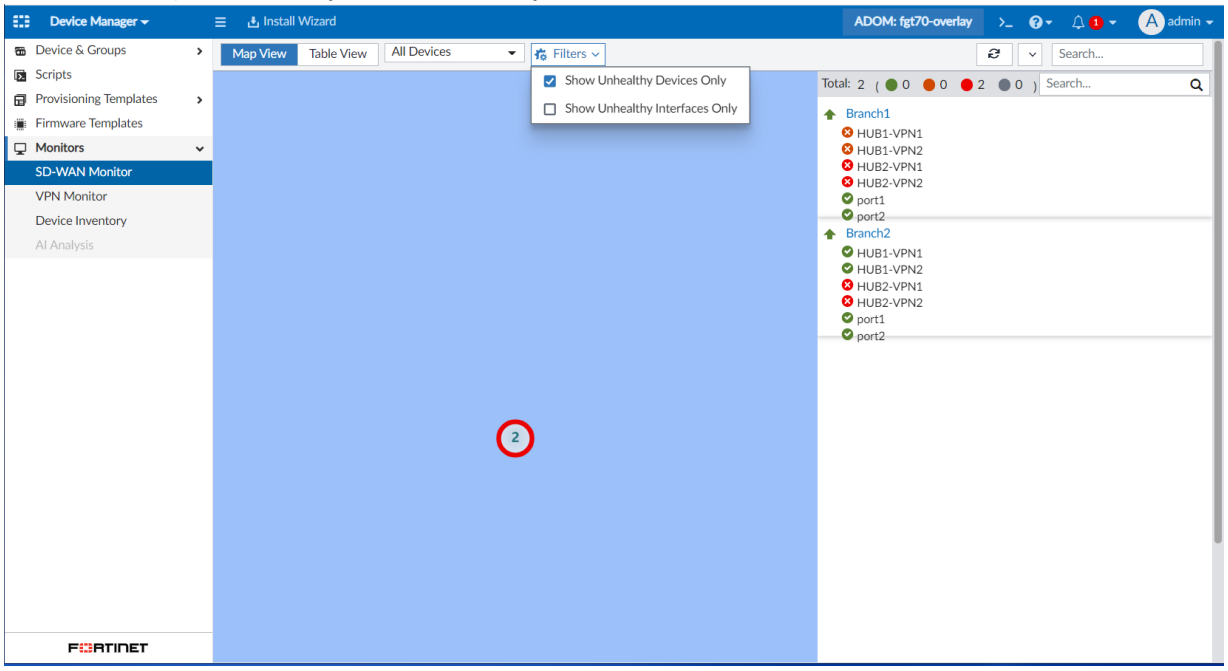

10. When complete, you can deploy the SD-WAN provisioning templates in your environment.

## SD-WAN Monitor includes new filter to display unhealthy devices or interfaces only - 7.2.1

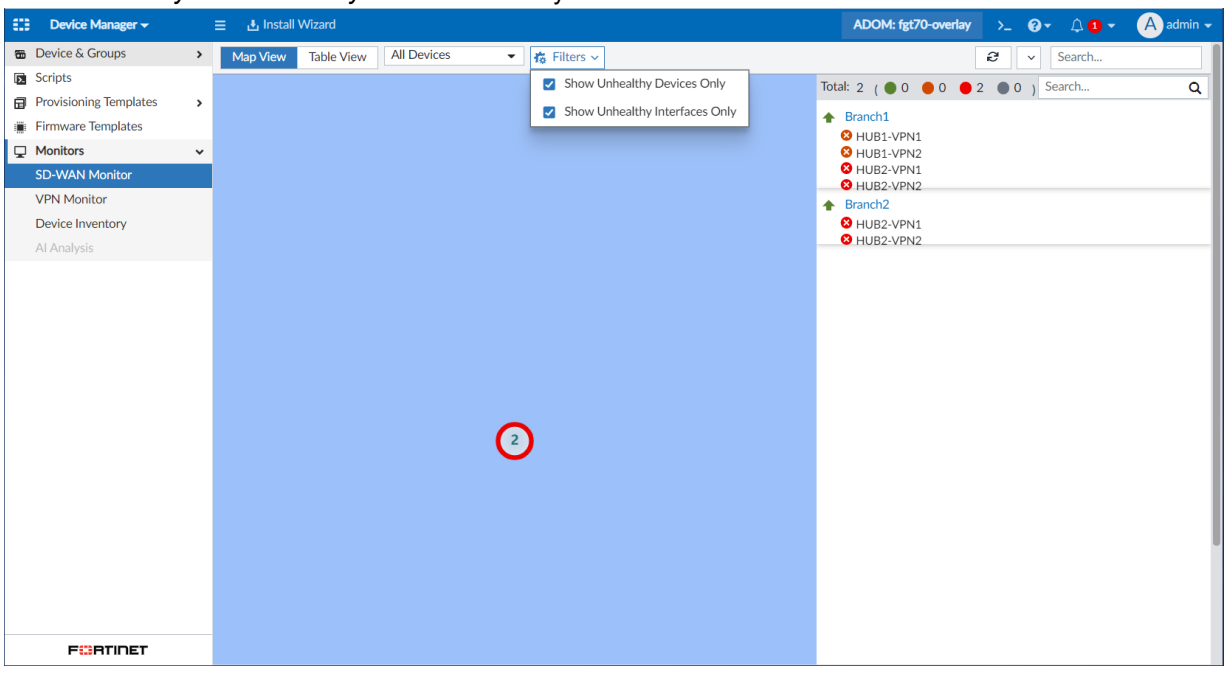
SD-WAN Monitor includes new filters to display unhealthy devices or interfaces only.

**To filter by unhealthy devices or interfaces only:**

1. Go to *Device Manager* > *Monitors* > *SD-WAN Monitor*.
2. Select the *Filters* dropdown. Two options are displayed:
   - *Show Unhealthy Devices* Only: Shows unhealthy devices not in the SLA and hides all others.

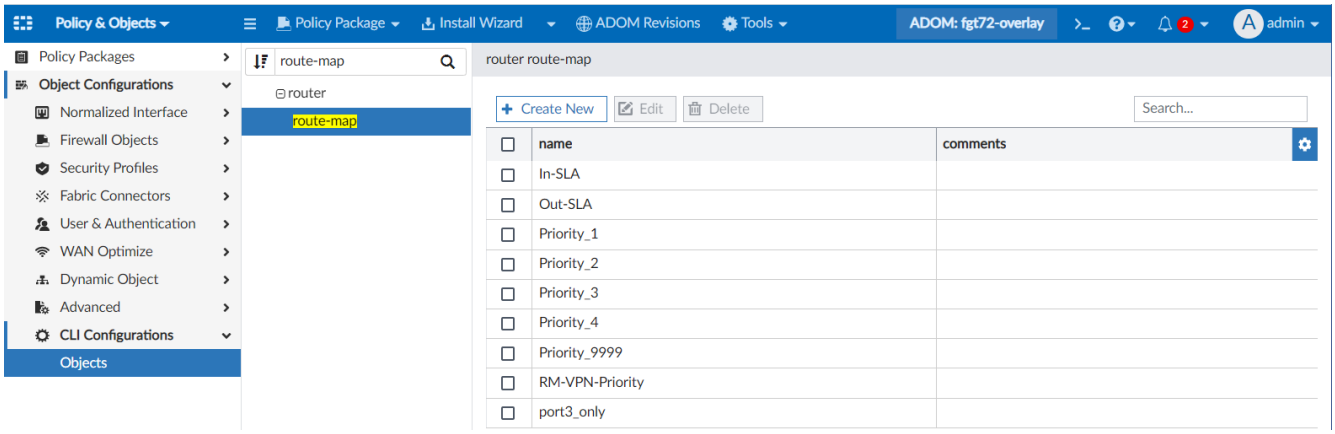



   - *Show Unhealthy Interfaces Only*: Shows unhealthy interfaces not in the SLA and hides all others.



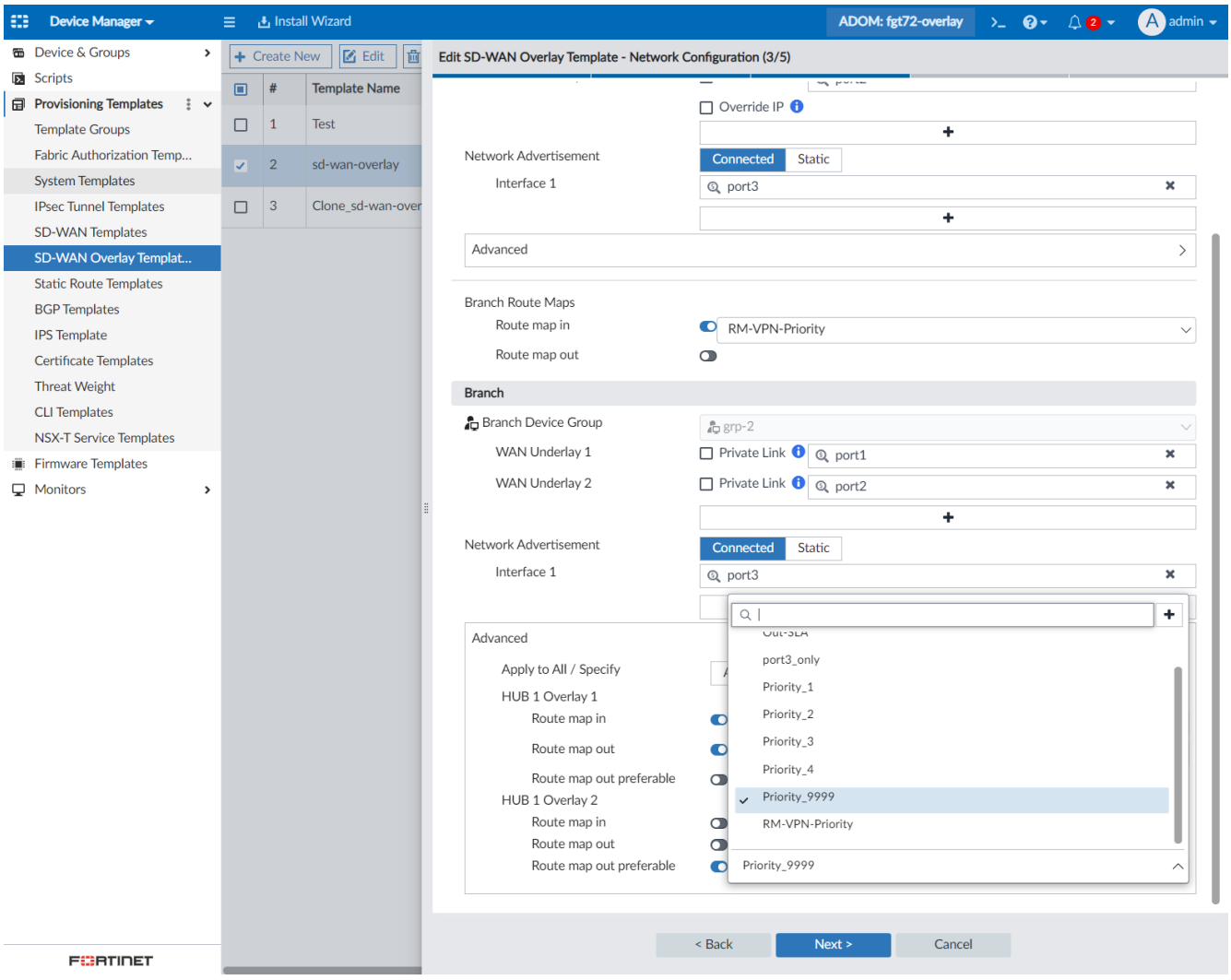
## Pre-built route-maps used for SD-WAN self-healing with BGP routing - 7.2.2

FortiManager 7.2.2 includes pre-built route-maps used for SD-WAN self-healing with BGP routing.

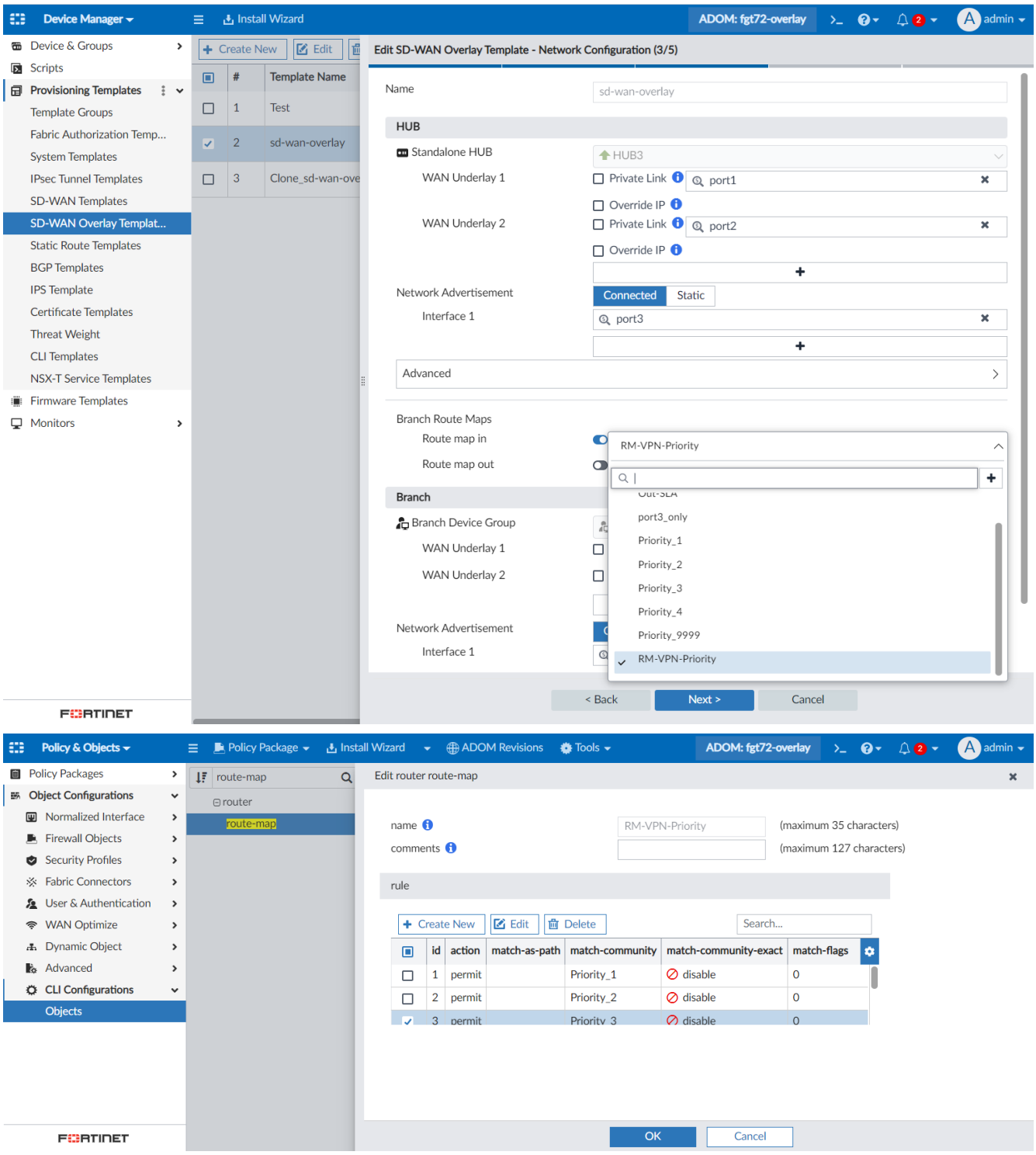



An option is available in the *SD-WAN Overlay Template* to automatically configure BGP neighbors based on HUB overlays and SLAs created by the overlay template.

The branch includes five (5) preconfigured route maps that the user may select, including: *Priority_1*, *Priority_2*, *Priority_3*, *Priority_4*, *Priority_9999* (used as a catch-all) and *RM-VPN-Priority*. Each route map will advertise a given community based on the *SD-WAN Overlay Template AS*.




Each HUB maps the route map to a priority. Established by the advertised community from the branch (based on the SLA information), the priority value will decide the preferred routing.

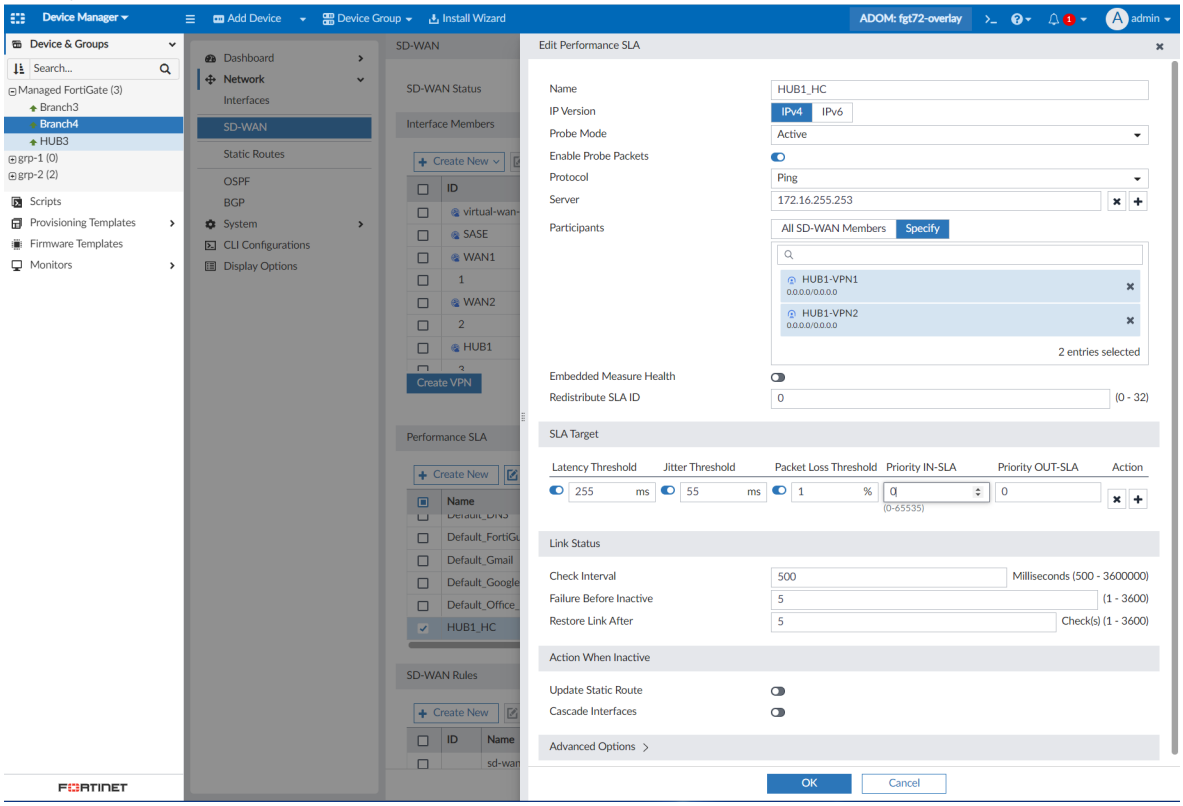



## SD-WAN Template added the health-check embedded SLA information - 7.2.2

SD-WAN Template added the health-check embedded SLA information used to avoid asymmetric routing on the return traffic.

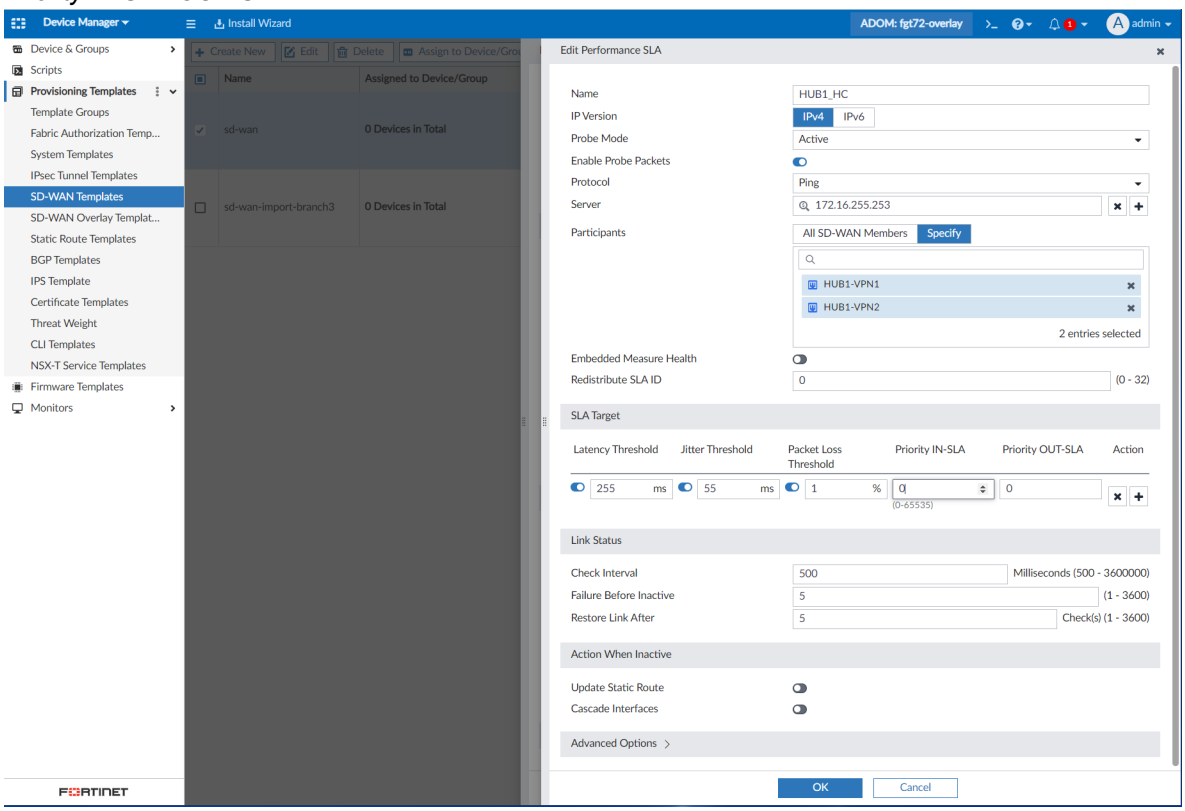
**To view the new settings in FortiManager:**

1. Enter a FortiManager 7.2 ADOM.
2. Go to *Device Manager* > *Managed Devices*, and select a managed device.
3. In the device database, go to *Network* > *SD-WAN*, and configure a *Performance SLA*.
   The following settings have been added:
   - Detection Mode: *Remote*
   - *Embedded Health Measure*
   - *Redistribute SLA ID*
   - *Priority IN-SLA/OUT-SLA*

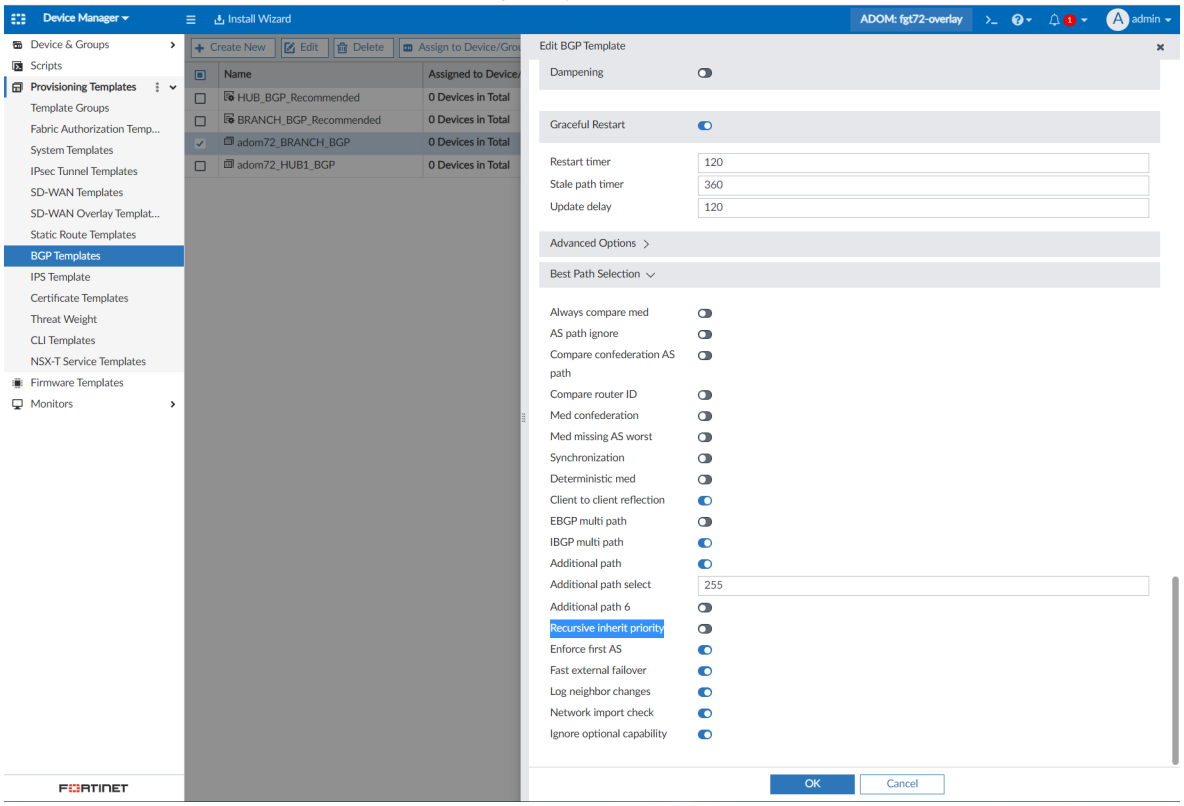



4. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*.
5. Edit or create an SD-WAN template.
6. Edit a *Performance SLA*.
   The following settings have been added:
   - Detection Mode: *Remote*
   - *Embedded Health Measure*
   - *Redistribute SLA ID*

- *Priority IN-SLA/OUT-SLA*




**7.** Go to *Device Manager* > *Provisioning Templates* > *BGP Templates*.
Under *Best Path Selection*, *Recursive inherit priority* has been added.



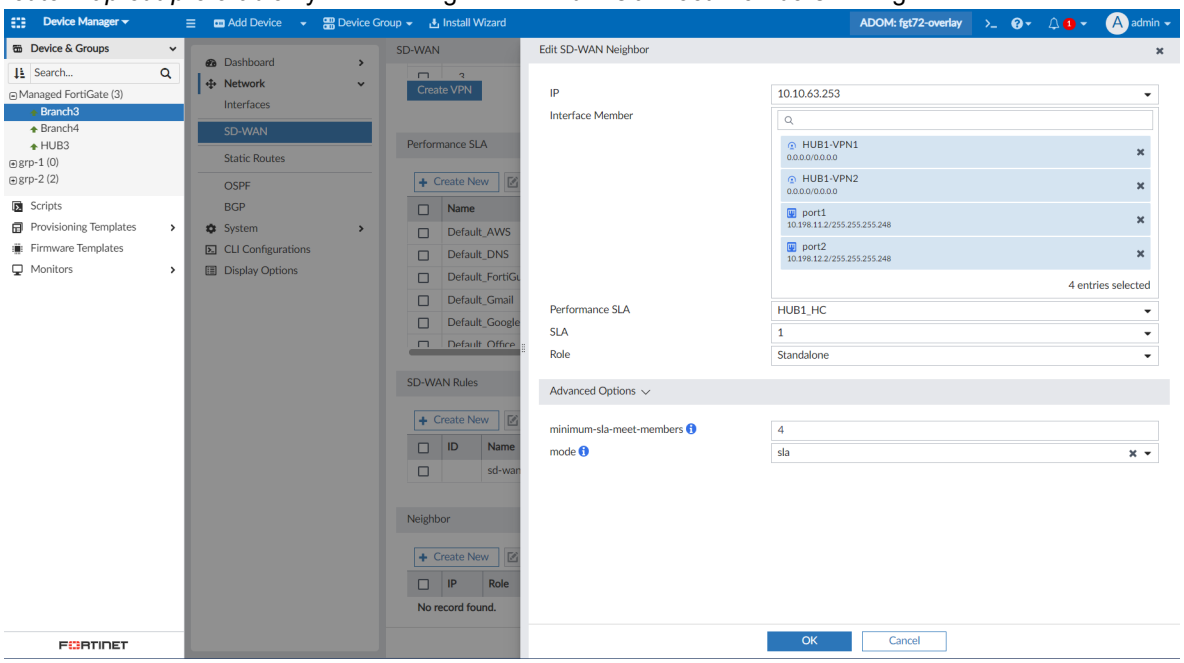
## FortiManager supports multiple interface members in the SD-WAN neighbor configurations - 7.2.2

FortiManager supports multiple interface members in the SD-WAN neighbor configurations.

This setting can be configured per-device configuration or using an SD-WAN Templates.

**To configure per-device:**

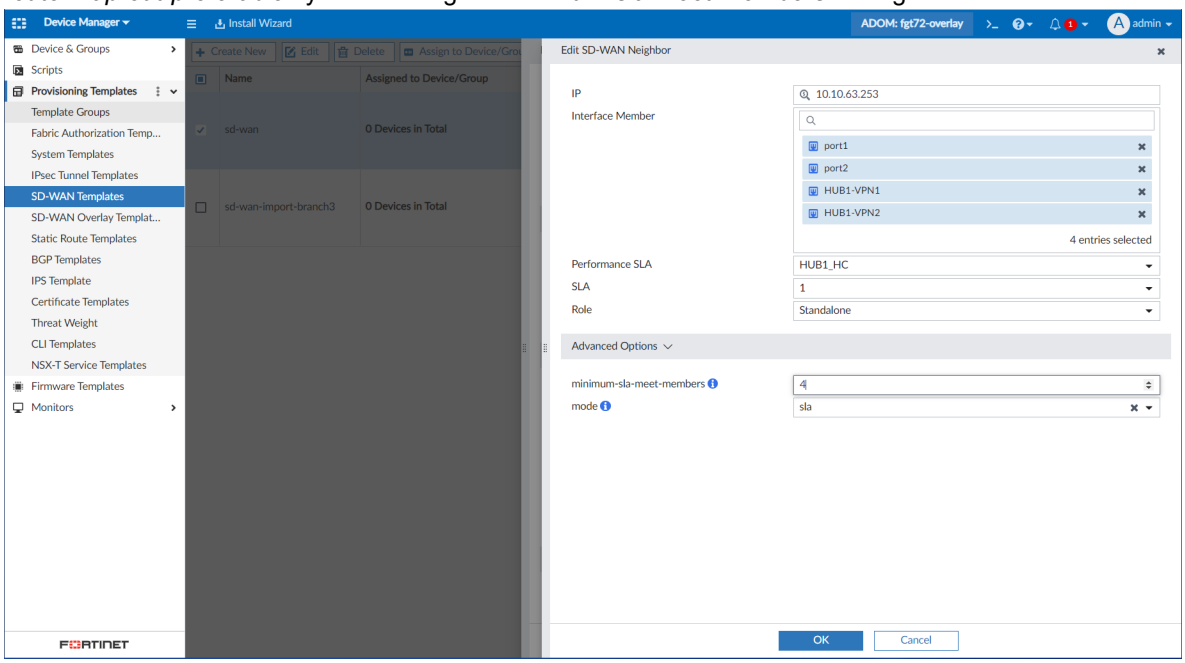
1. In a FortiManager 7.2 ADOM, go to *Device Manager* > *Managed Devices*, and select a managed device.
2. In the device database, go to *Network* > *SD-WAN*, and create or edit a *Neighbor*.Multiple *Interface Members* can be configured.
3. Open *Advanced Options*. You can configure the minimum number of members that needs to be in SLA to utilize *route-map-out-preferable* by customizing the *minimum-sla-meet-members* setting.




**To configure using an SD-WAN Template:**

1. In a FortiManager 7.2 ADOM, go to *SD-WAN Templates*, and edit or create a template.
2. Edit an *SD-WAN Neighbor*. Multiple *Interface Members* can be configured.

3. Open *Advanced Options*. You can configure the minimum number of members that needs to be in SLA to utilize *route-map-out-preferable* by customizing the *minimum-sla-meet-members* setting.




# Templates

This section lists the new features added to FortiManager for templates:


- SD-WAN template enhancement on page 53
- IPS template combines configuration for global "IPS Global" and per-vdom "System IPS " / "IPS Settings" on page 59
- Device blueprints on page 61
- CLI templates have increased visibility for troubleshooting on page 64
- Improved CLI templates with validation and preview functions on page 68
- Fabric Authorization Template automatically provisions and authorizes LAN Edge devices on the managed FortiGates 7.2.1 on page 74


## SD-WAN template enhancement

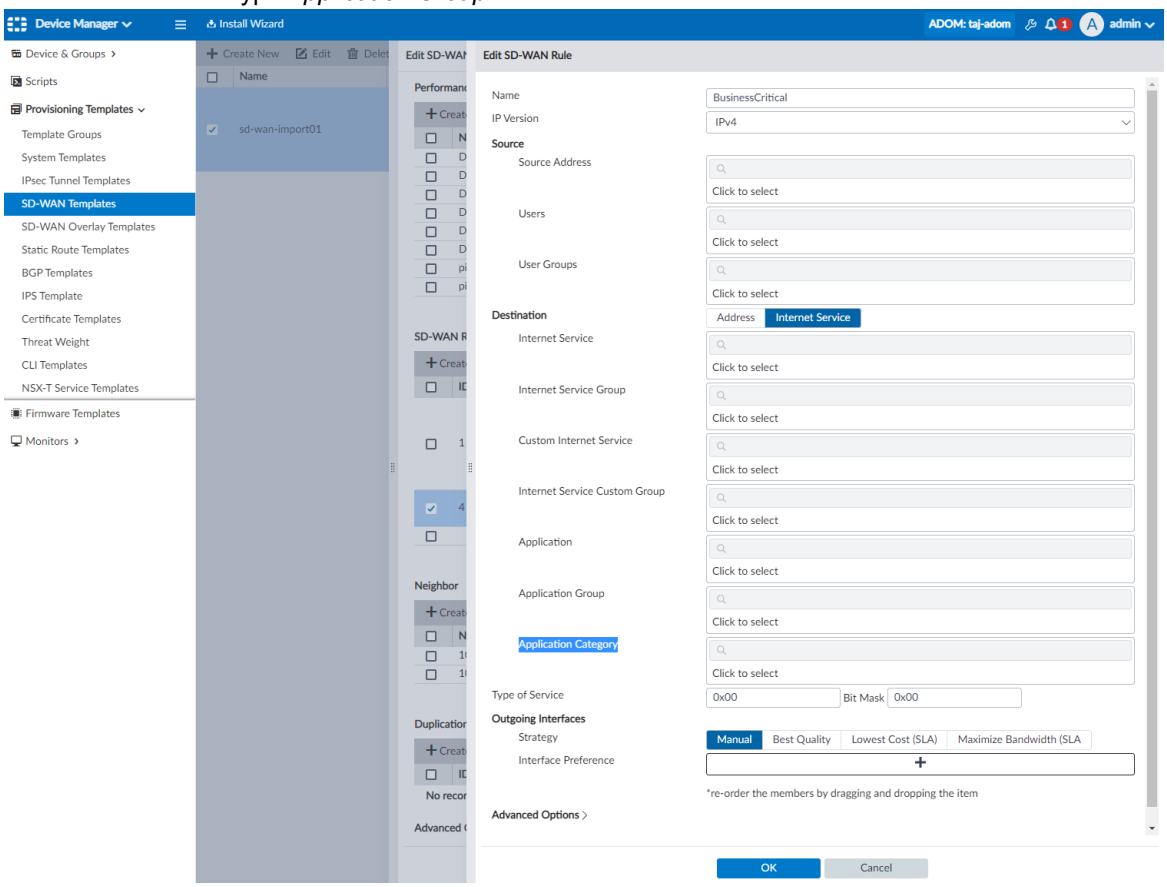
In FortiManager 7.2.0, SD-WAN templates have been enhanced to include the default FortiGuard applications and application groups categories.

The application category uses the default internet service database (ISDB) categories received from FortiGuard. This feature is available in a FortiManager 7.2 ADOM with 7.2 or later FortiGate devices.

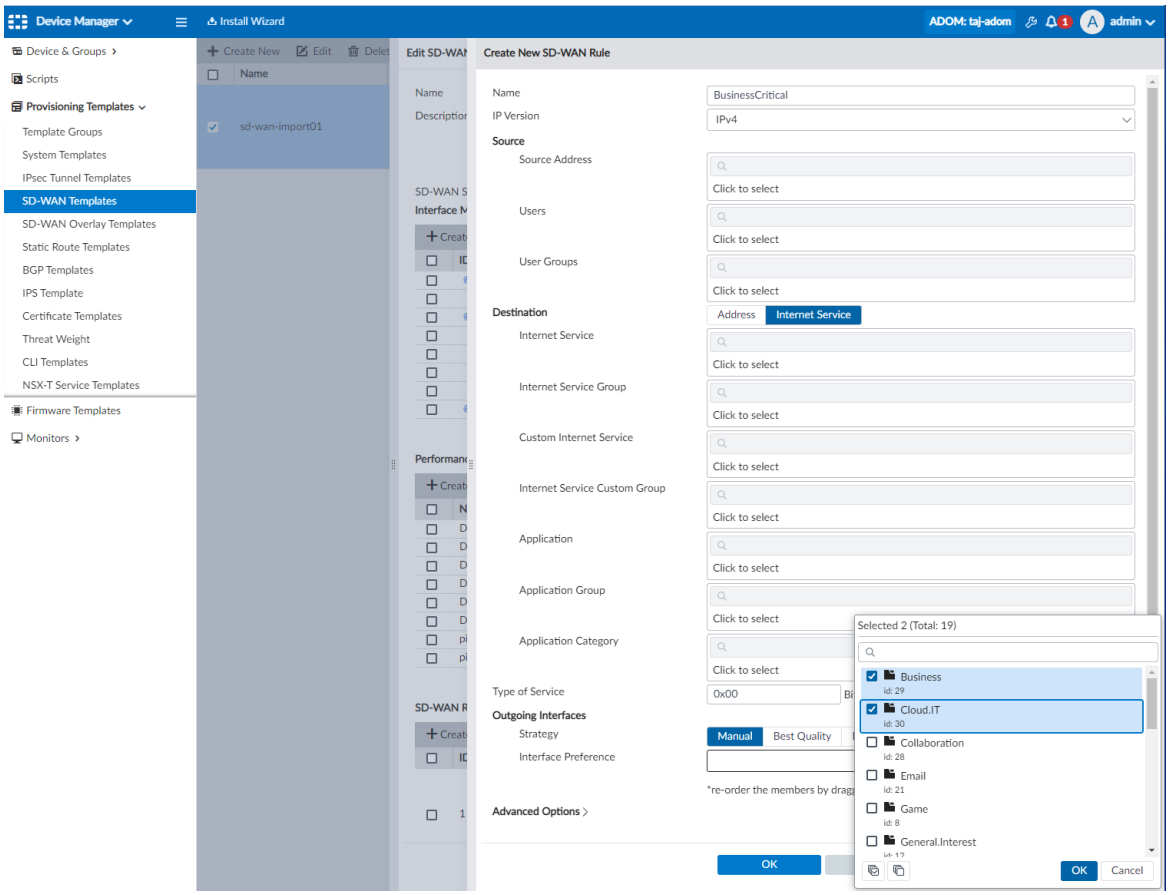
**To configure application groups for SD-WAN rules in a template:**

1. In FortiManager, make sure you're in a 7.2 ADOM.
2. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*, and create or edit a template.

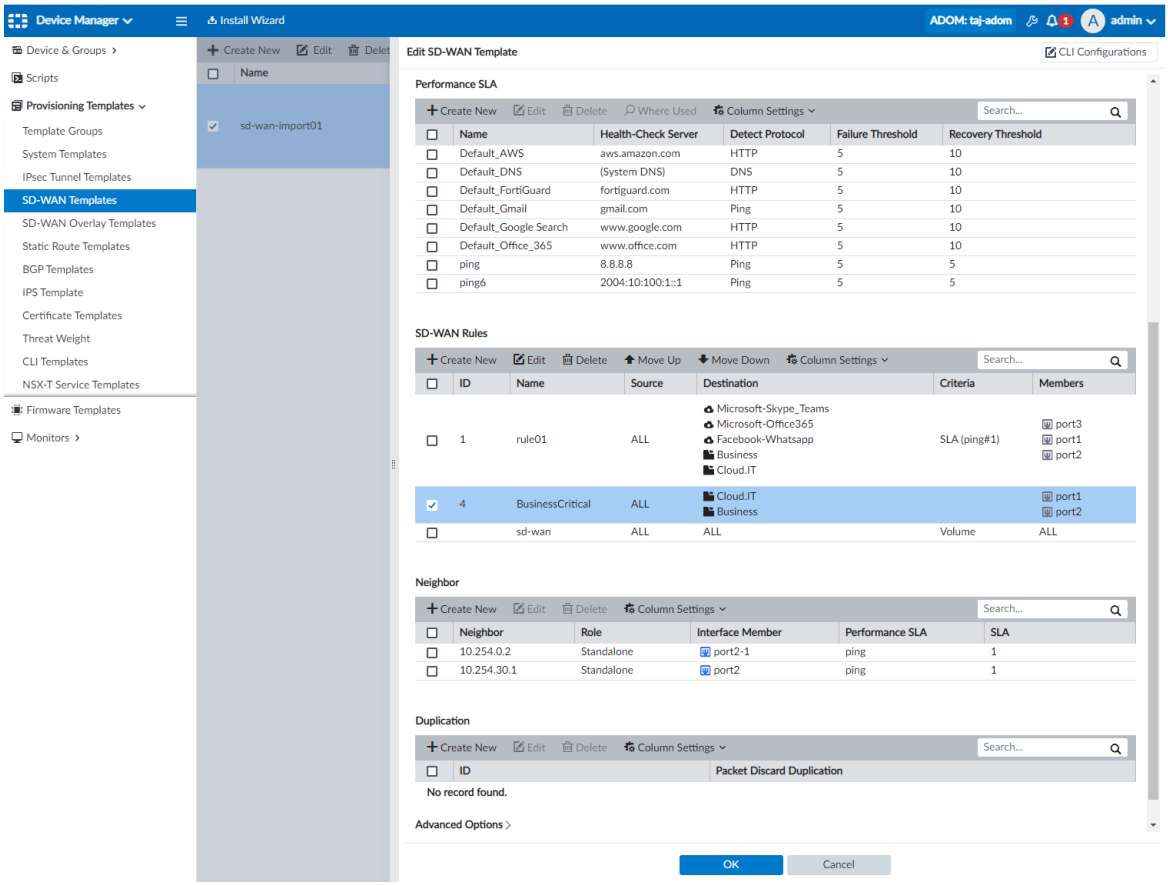
3. Under *SD-WAN Rules*, create a new rule.
4. Set the *Destination* as *Internet Service*.
   The new destination type *Application Group* has been added.



5. Select categories from the default ISDB list. New categories can be created by clicking the add button in the selection window.



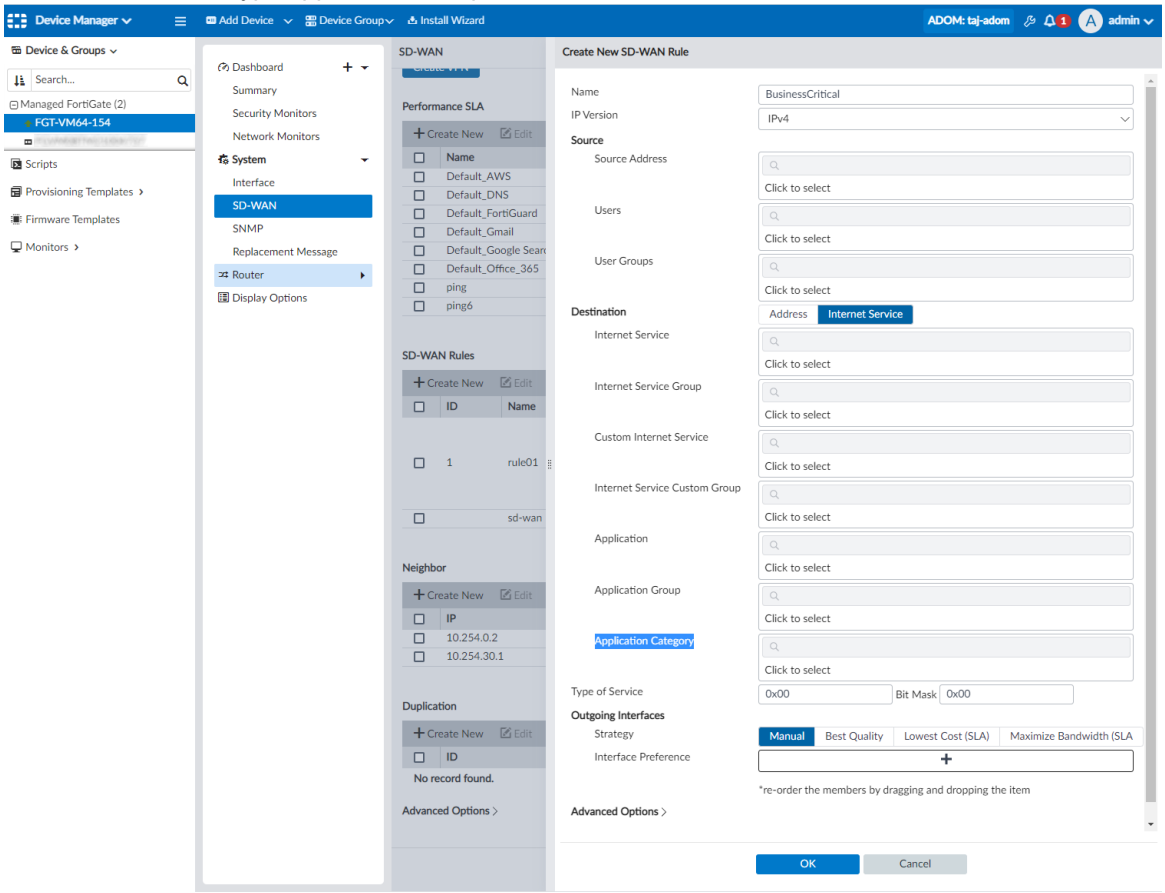
6. Click *OK* to save the SD-WAN rule.



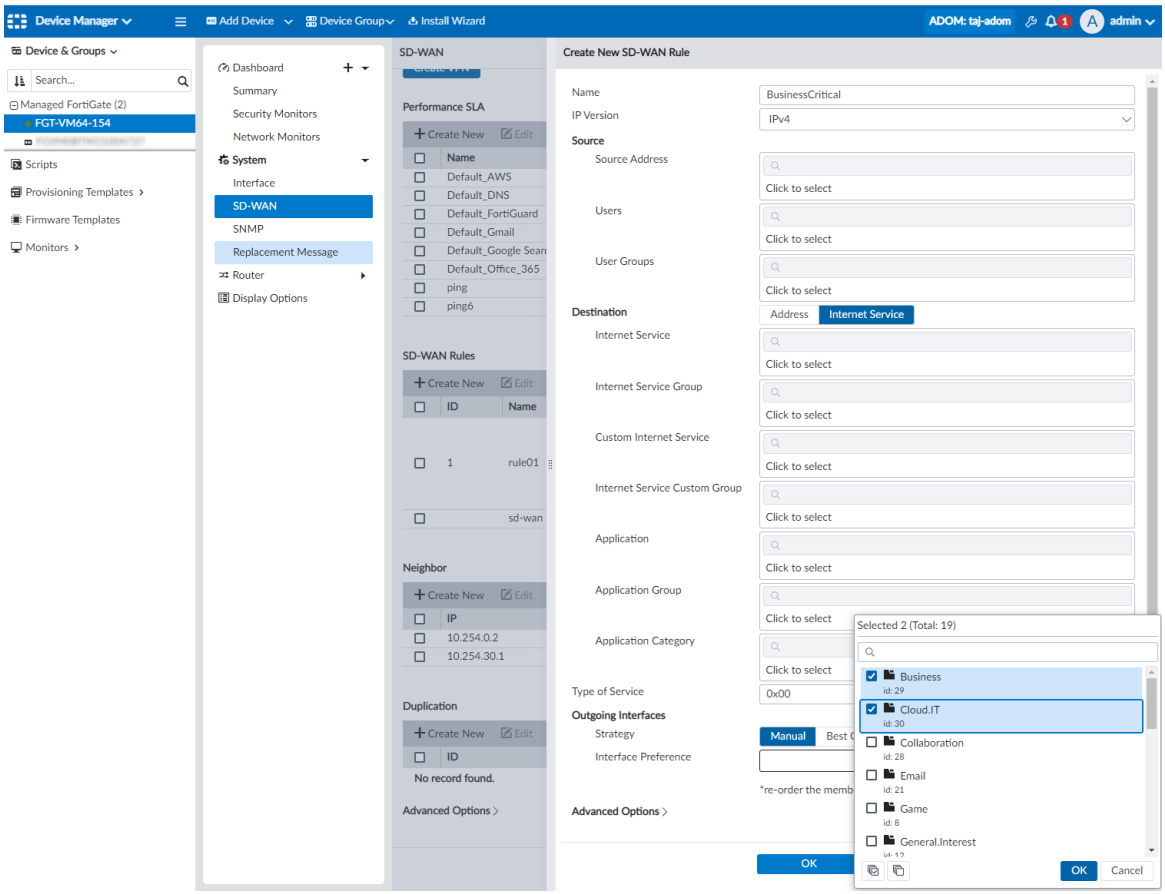

**To configure application groups for SD-WAN rules in the device database:**

1. In FortiManager, make sure you're in a 7.2 ADOM.
2. Go to *Device Manager* > *Device & Groups*.
3. Select a FortiGate device (7.2 or later) to manage the device database.
4. Go to *System* > *SD-WAN* > *SD-WAN Rules*, and create a new rule.

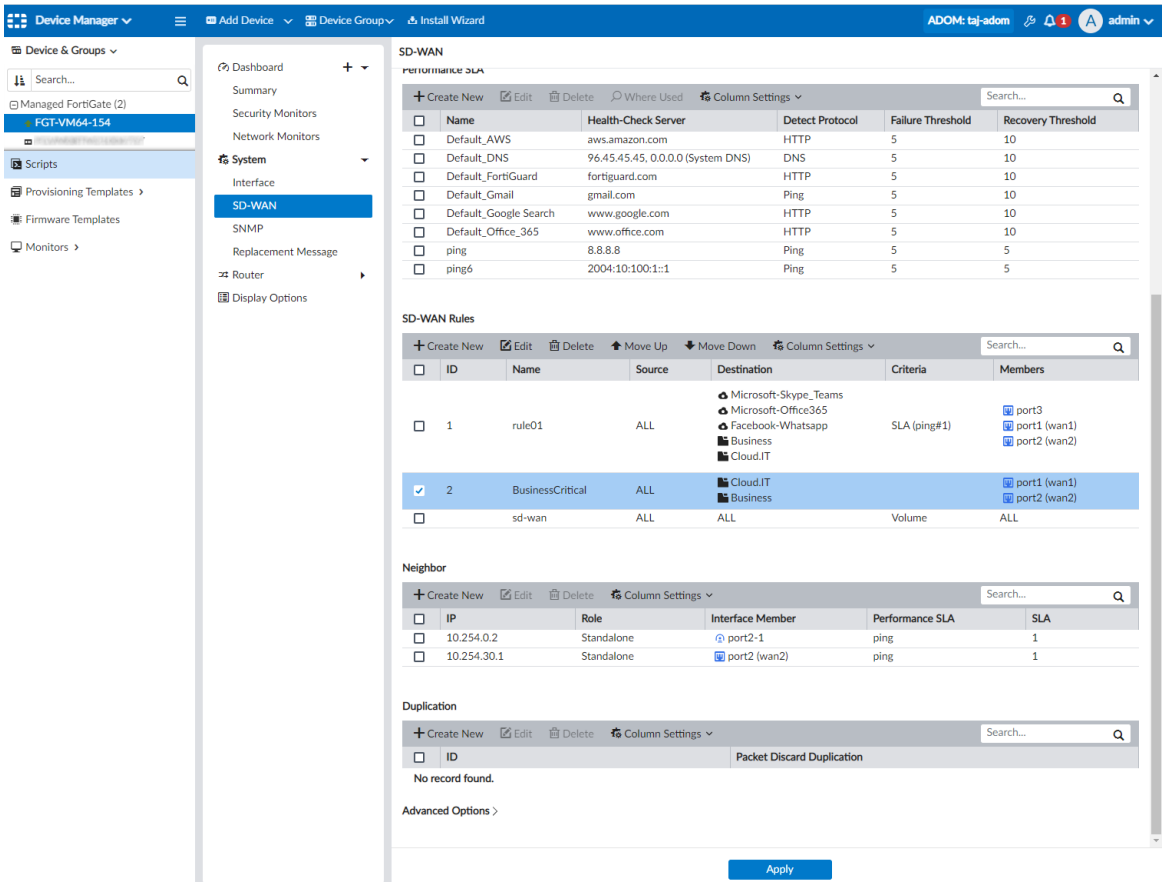
5. Set the *Destination* as Internet Service.
   The new destination type *Application Group* has been added.



6. Select categories from the default ISDB list. New categories can be created by clicking the add button in the selection window.



7. Click *OK* to save the SD-WAN rule.




## IPS template combines configuration for global "IPS Global" and per-vdom "System IPS " / "IPS Settings"

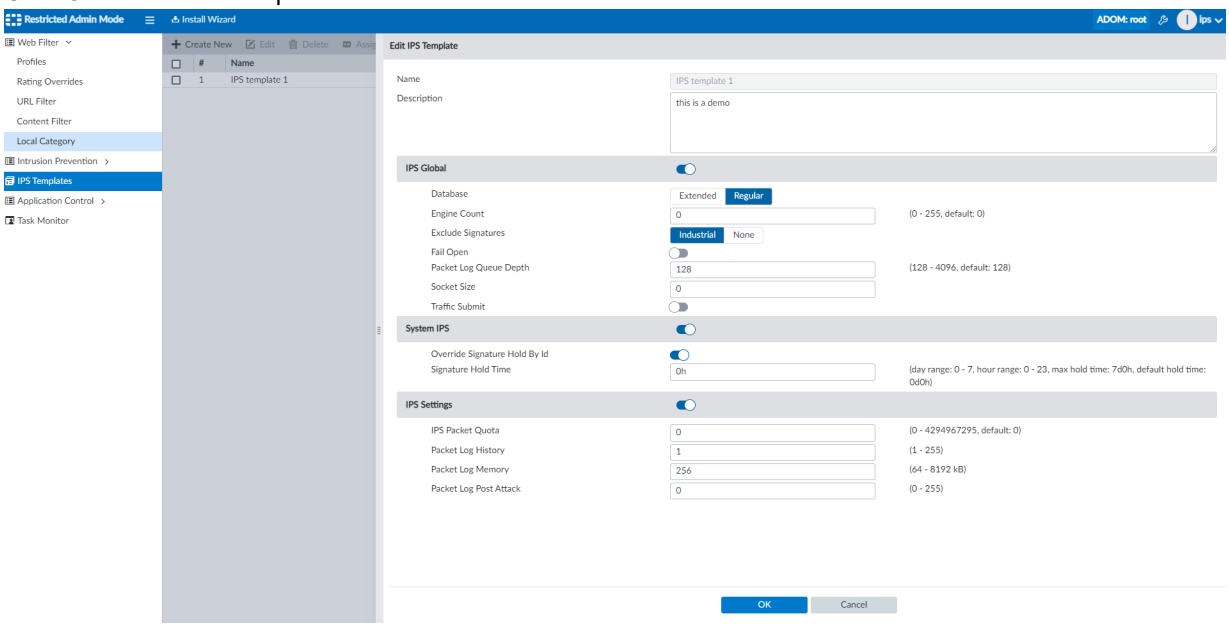
In FortiManager 7.2.0, a new IPS template is available.

The IPS template combines configuration for global "IPS Global" and per-vdom "System IPS " / "IPS Settings"

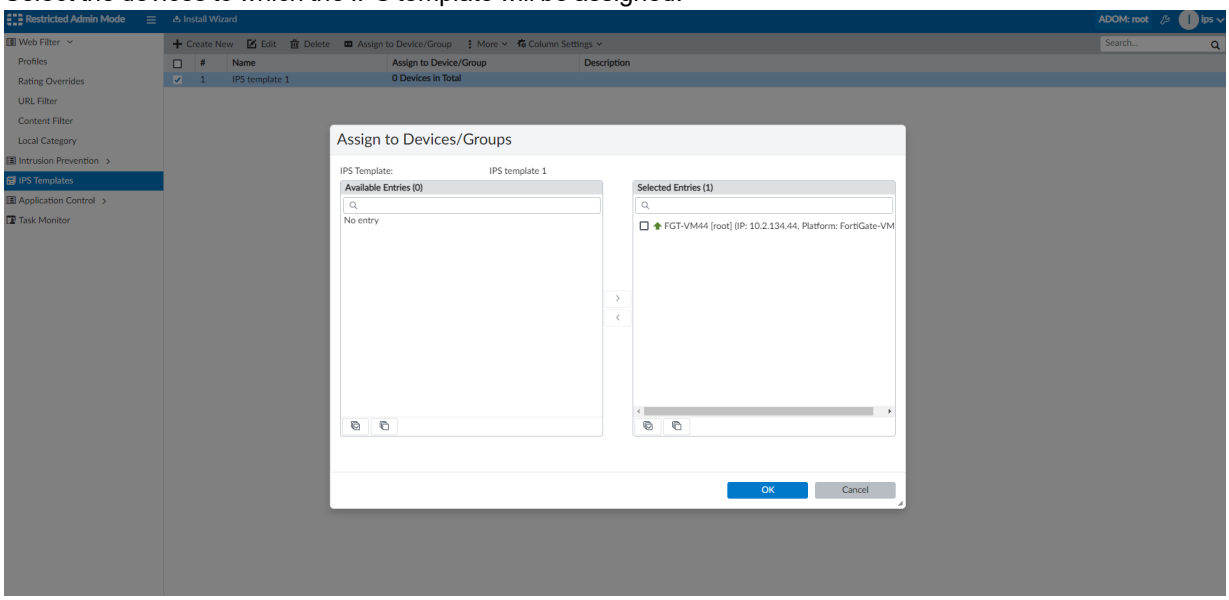
**To create an IPS template:**

1. As a restricted IPS administrator, go to *IPS Templates* in the tree menu.
2. Create the IPS template.
   a. Click *Create New* to create a new IPS template.
   b. Configure the details for your IPS template, including the *IPS Global*, *System IPS*, and *IPS Settings*.

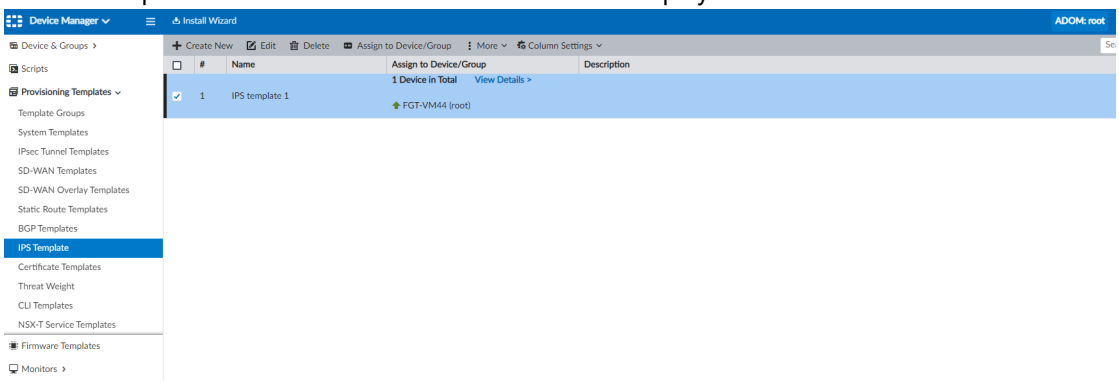
c. Click *OK* to save the template.




3. Assign the IPS template.
   a. In the IPS Template pane, click *Assign to Device/Groups*.
   b. Select the devices to which the IPS template will be assigned.



4. Check the IPS template in the Device Manager.
   a. As a non-restricted administrator, go to the FortiManager *Device Manager* > *IPS Template*.
   b. The ISP template created as a restricted administrator is displayed.




## Device blueprints

In FortiManager 7.2.0, you can create device blueprints to simplify configuration of certain device settings, including device groups, configuring pre-run templates, policy packages, provisioning templates, and more. Once a device blueprint has been created, it can be selected when adding a model device or when importing multiple model devices from a CSV file.

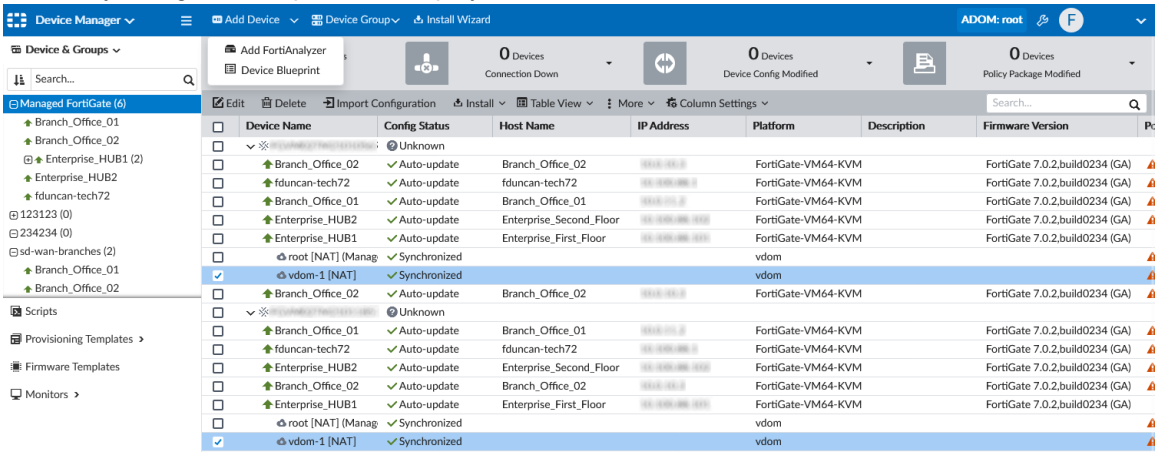
The following information is available:

- Creating a device blueprint on page 61
- Adding model devices using a blueprint on page 62

### Creating a device blueprint

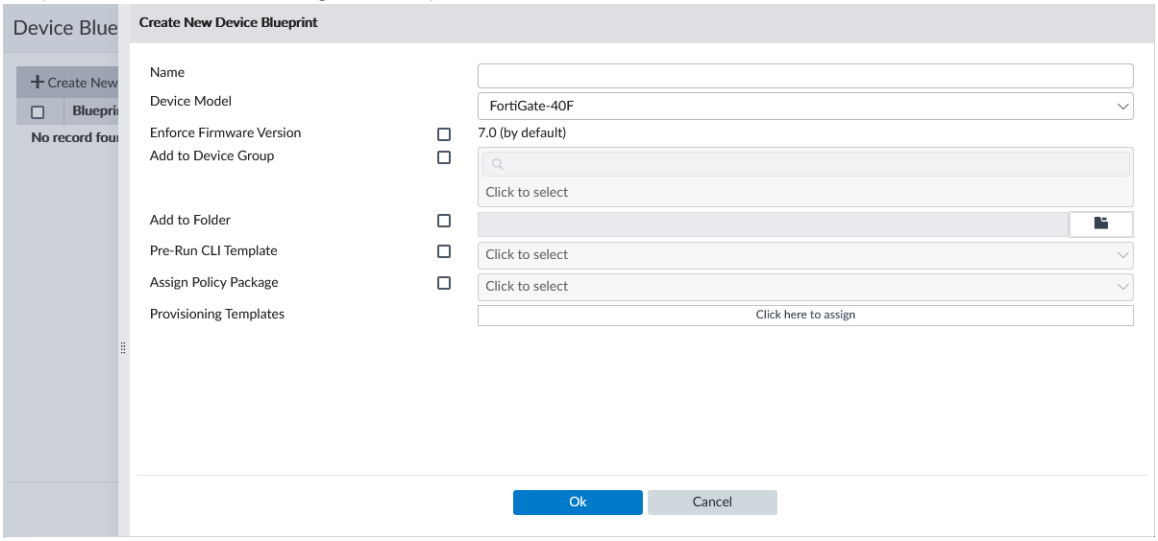
**To create a new device blueprint:**

1. Go to Device Manager, and select *Device Blueprint* from the *Add Device* dropdown menu. Previously configured blueprints are displayed in the table below and can be edited or deleted.




2. Click *Create New* to add a new blueprint.
3. Select the model devices to which the blueprint can be applied.

4. Configure the device setting details for the blueprint. For example, you can specify a device group and provisioning template for the devices using this blueprint.

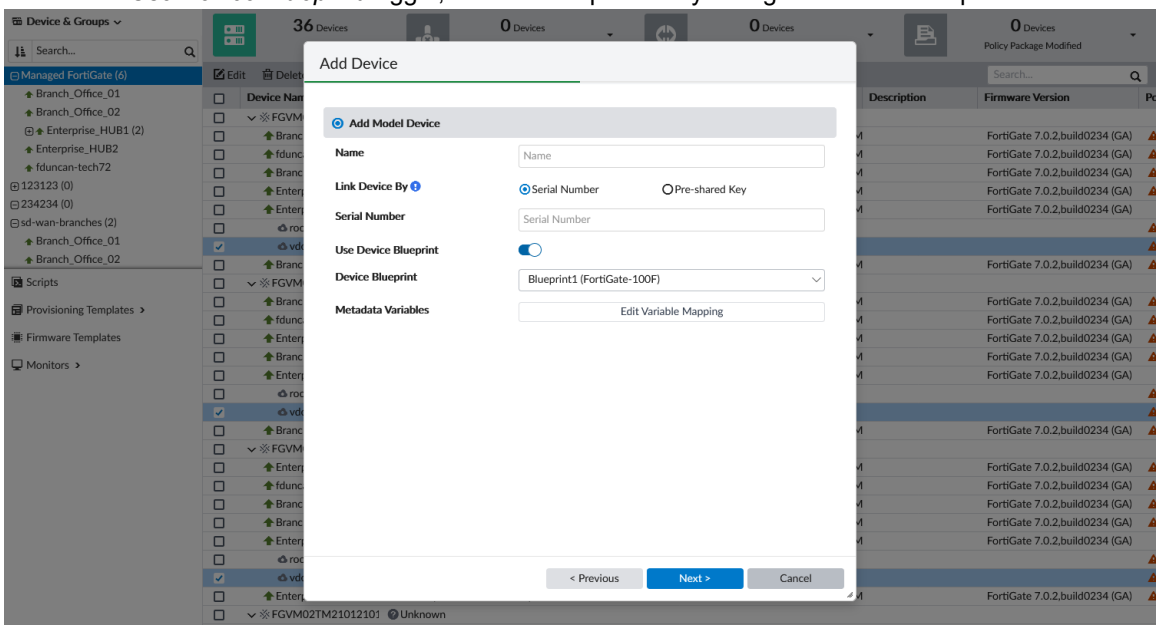



5. Click *OK*.

## Adding model devices using a blueprint

**To use a blueprint when adding a model device:**

1. Go to *Device Manager* > *Device & Groups*.
2. Click *Add Device*. The *Add Device* wizard displays.
3. Click *Add Model Device*.
   The Add Device window is displayed.
4. Enter the name and serial number or pre-shared key for the device.
5. Enable the *Use Device Blueprint* toggle, and select a previously configured device blueprint.

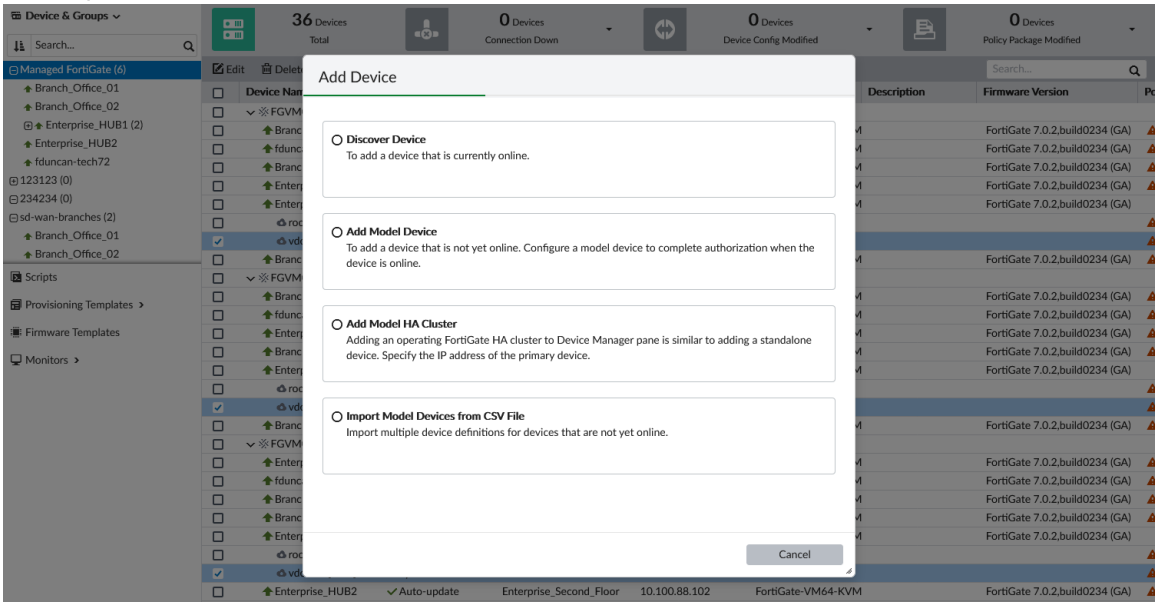


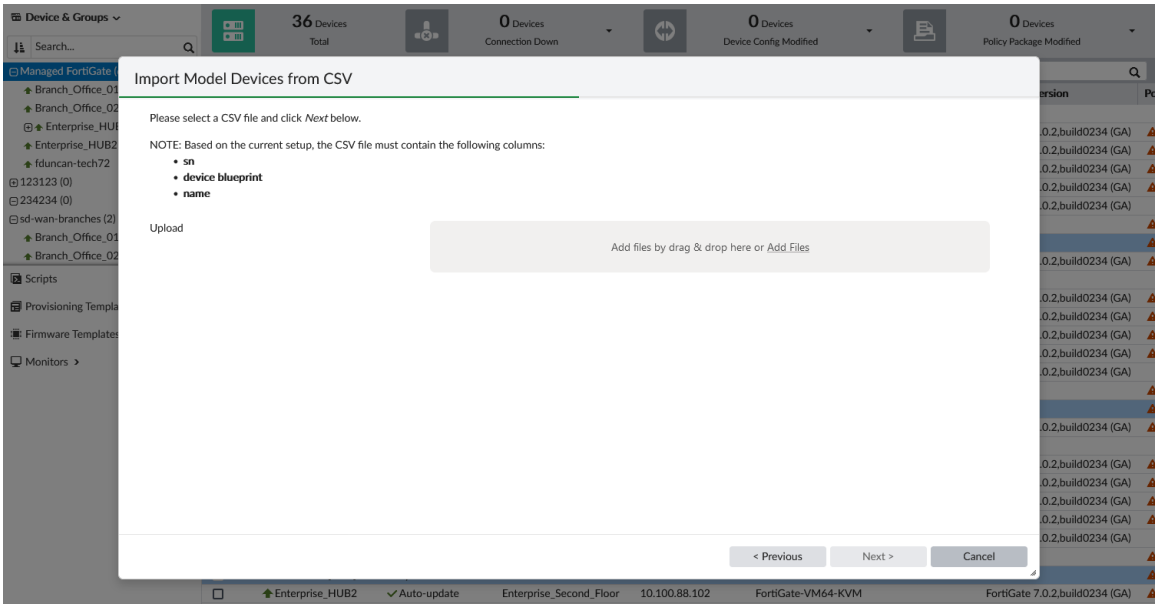

You can alternatively click the add icon to create a new device blueprint.

6. Optionally, configure the metadata variables for this device.
7. Click *Next* to continue importing the device.

**To import model devices from a CSV File:**

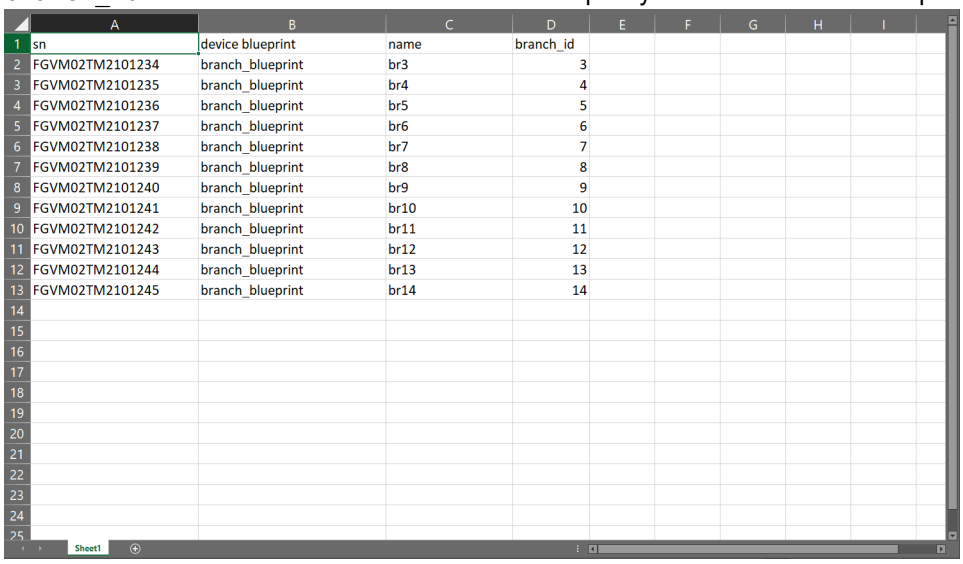
1. If ADOMs are enabled, select the ADOM to which you want to add the device.
2. Go to *Device Manager* > *Device & Groups*.
3. Click *Add Device*.
   The Add Device window is displayed.
4. Click *Import Model Devices from CSV File*.




5. Configure your local CSV file for the devices that you want to import. CSV files must contain the following columns: `sn`, `device blueprint`, and `name`, with the respective data listed in the cells below.
   Additional columns can be added for each metadata variable that you want to specify. In the following image, the

`branch_id` metadata variable has been added to specify this variable for each imported device.



| | A | B | C | D |
|---|---|---|---|---|
| 1 | sn | device blueprint | name | branch_id |
| 2 | FGVM02TM2101234 | branch_blueprint | br3 | 3 |
| 3 | FGVM02TM2101235 | branch_blueprint | br4 | 4 |
| 4 | FGVM02TM2101236 | branch_blueprint | br5 | 5 |
| 5 | FGVM02TM2101237 | branch_blueprint | br6 | 6 |
| 6 | FGVM02TM2101238 | branch_blueprint | br7 | 7 |
| 7 | FGVM02TM2101239 | branch_blueprint | br8 | 8 |
| 8 | FGVM02TM2101240 | branch_blueprint | br9 | 9 |
| 9 | FGVM02TM2101241 | branch_blueprint | br10 | 10 |
| 10 | FGVM02TM2101242 | branch_blueprint | br11 | 11 |
| 11 | FGVM02TM2101243 | branch_blueprint | br12 | 12 |
| 12 | FGVM02TM2101244 | branch_blueprint | br13 | 13 |
| 13 | FGVM02TM2101245 | branch_blueprint | br14 | 14 |

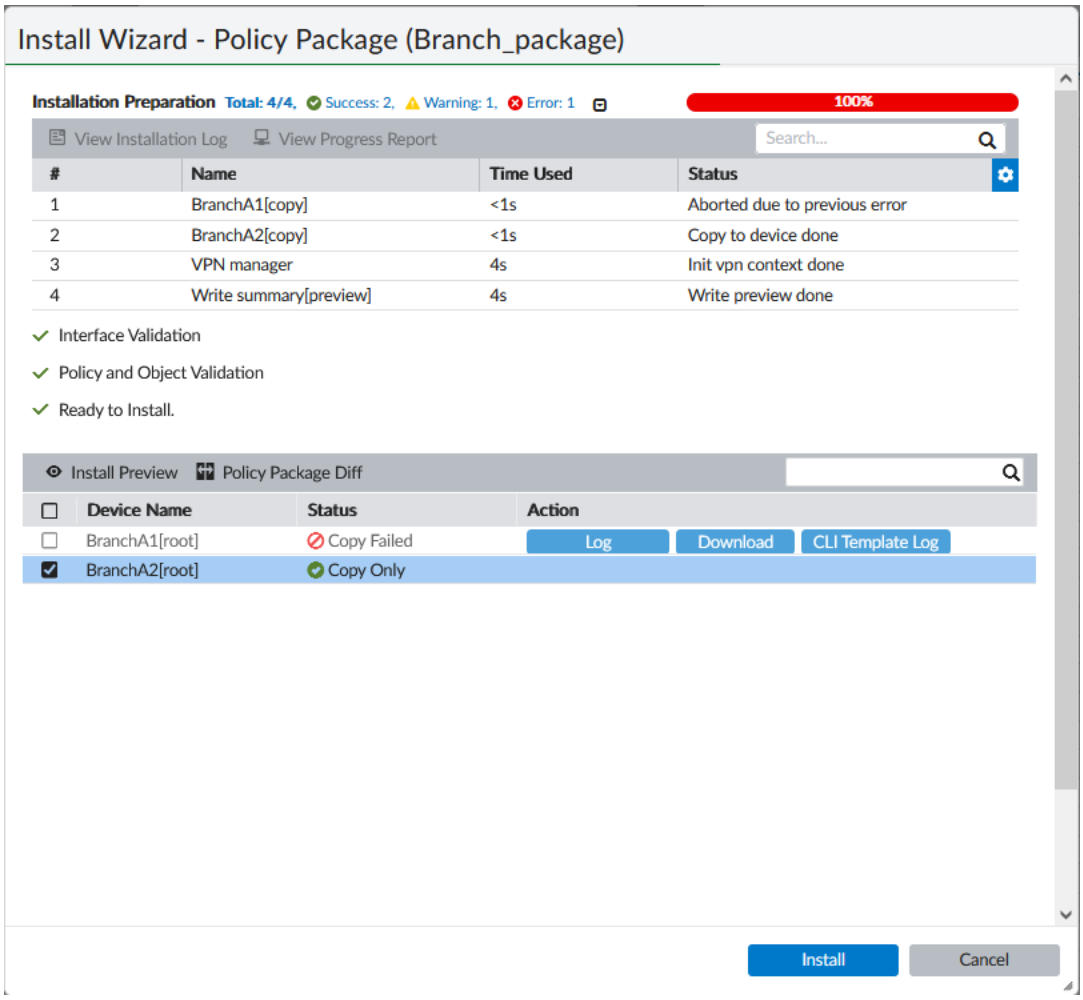
6. Drag and drop the CSV file into the *Upload* area, or select the CSV file location on your computer.
   The model devices' serial numbers, names, blueprints, and optional metadata variables are displayed in the table.
7. Review the device list, and click *Next* to begin importing the devices.
8. Click *Finish* when the import process is complete.

## CLI templates have increased visibility for troubleshooting

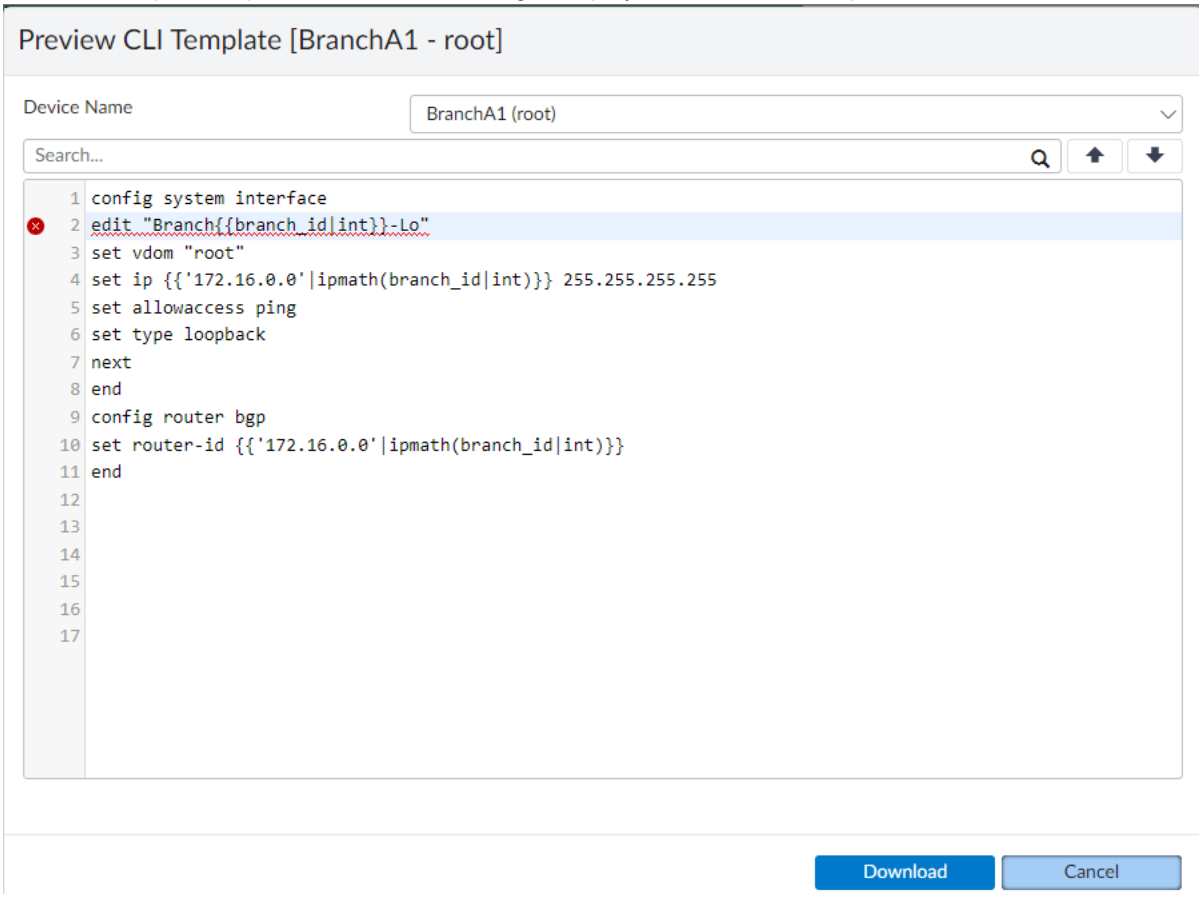
CLI templates have increased visibility for troubleshooting including: line numbering, detailed error report with line number, template name, and reason for the installation failure.

**To view CLI template improvements for troubleshooting:**

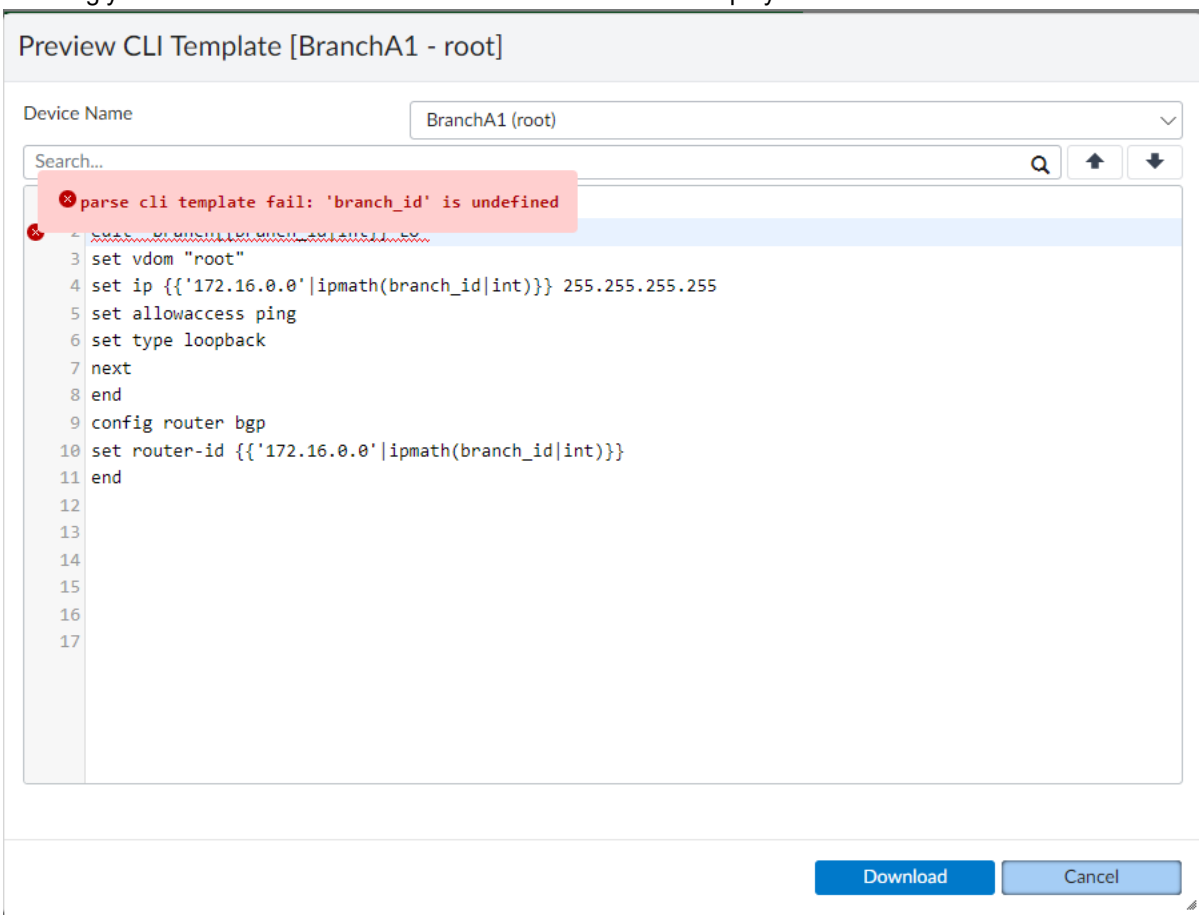
1. In this example, performing a policy package install for two devices encounters a *Copy Failed* error for FortiGate "BranchA1."


Install Wizard - Policy Package (Branch_package)
Installation Preparation Total: 4/4, Success: 2, Warning: 1, Error: 1
100%
View Installation Log
View Progress Report
Search...
# Name Time Used Status
1 BranchA1[copy] <1s Aborted due to previous error
2 BranchA2[copy] <1s Copy to device done
3 VPN manager 4s Init vpn context done
4 Write summary[preview] 4s Write preview done
Interface Validation
Policy and Object Validation
Ready to Install.
Install Preview
Policy Package Diff
Device Name Status Action
BranchA1[root] Copy Failed Log Download CLI Template Log
BranchA2[root] Copy Only
Install
Cancel

2. Click *CLI Template Log* , and the *Preview* dialog is displayed with the CLI template content.

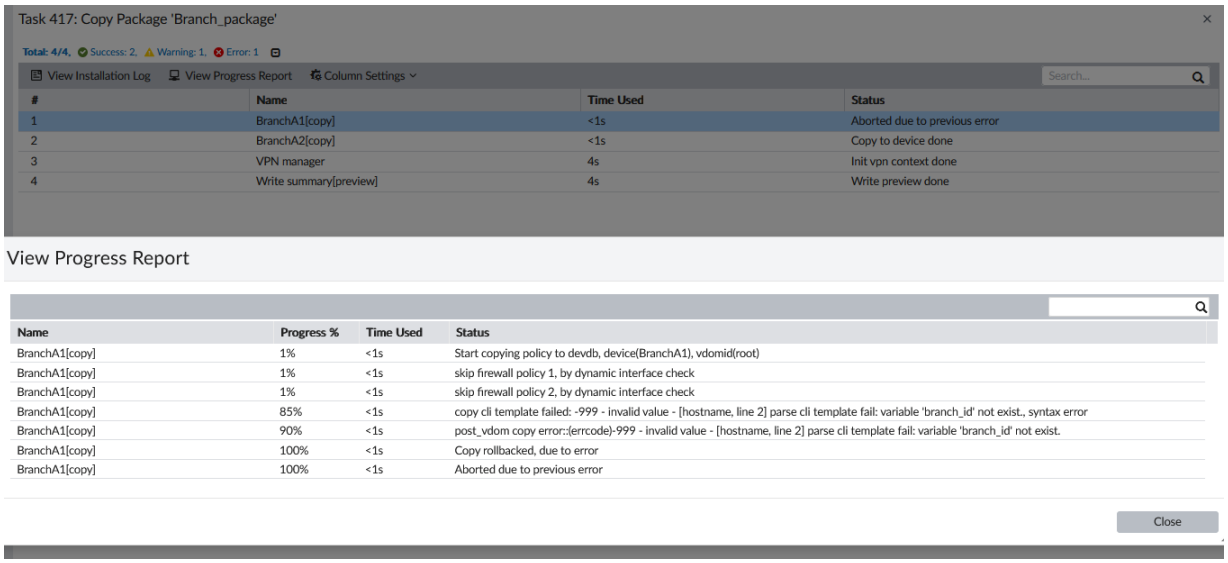


3. Hovering your mouse over the red x where an error is indicated displays information about the error.




4. After the installation is finished, information is displayed in the task monitor. Double click on a task ID and select *View Progress Report*.
   In this example, the progress report for FortiGate BranchA1 includes the following information:
   - The CLI template name: Hostname
   - The line number: 2

- The reason the copy failed: branch_id not exist, syntax error




## Improved CLI templates with validation and preview functions

Improved CLI templates with *Validation* and *Preview* functions, to perform verification of the template before installation. Metadata variables used in CLI templates (including Jinja variables) can be imported/exported from/to a JSON file.

This topic includes the following sections:

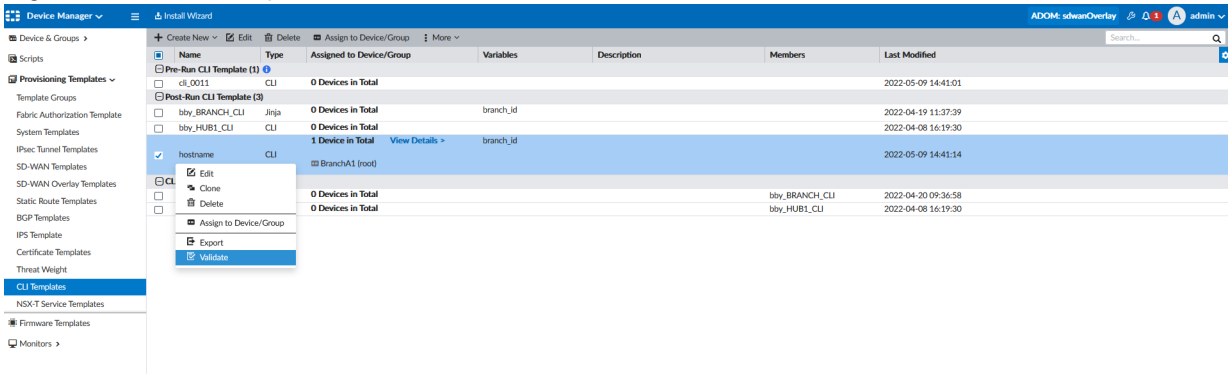


For an example of how these features can be used while configuring SD-WAN, IPsec and BGP for branch offices using the CLI template, see the following: Branch configuration using FortiManager Jinja2 CLI templates on page 247

## CLI template validation

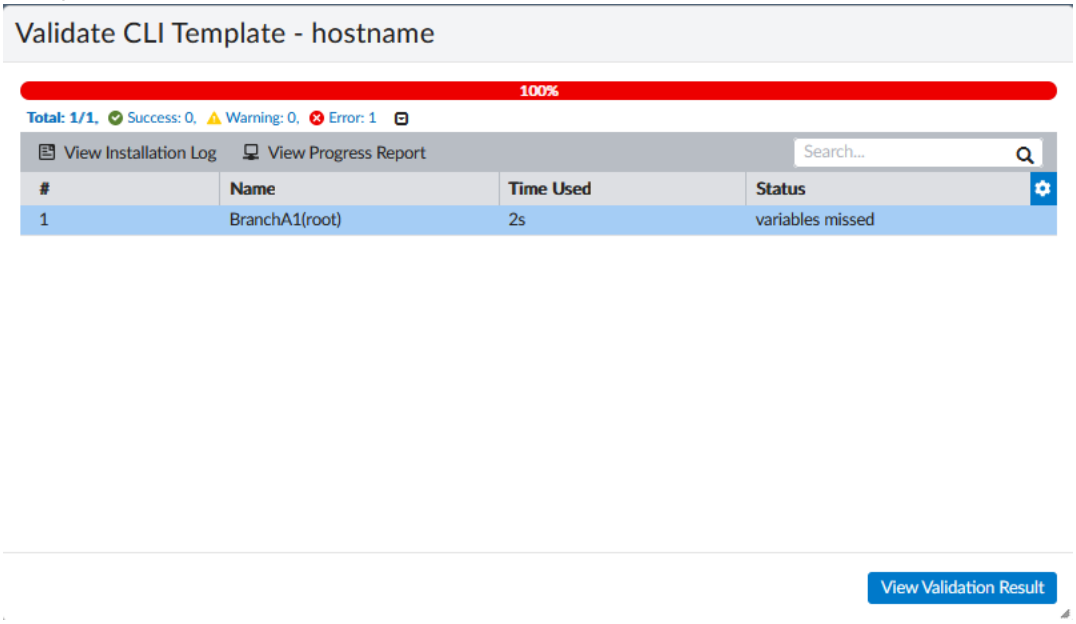
**To validate CLI templates:**

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Templates*.
2. Right-click on a CLI template, and select *Validate* from the menu.

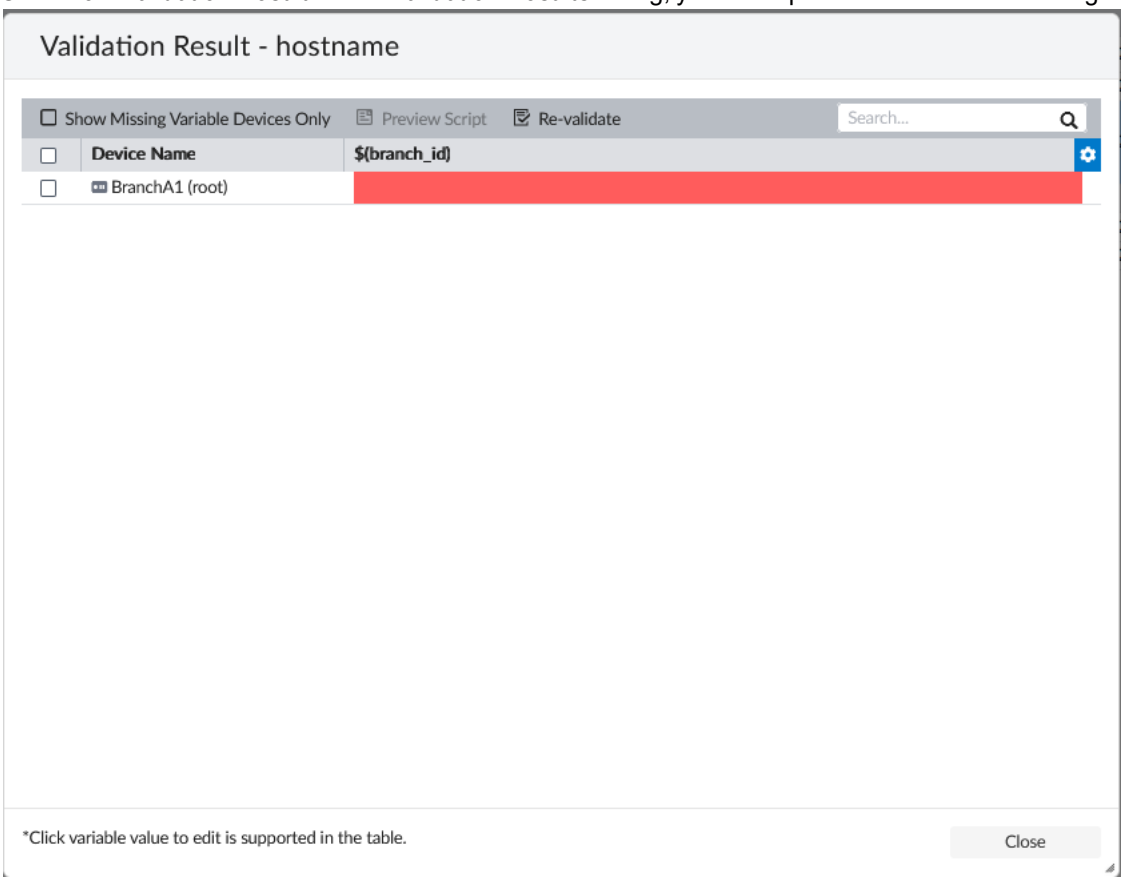



The *Validate CLI Template* dialog appears.

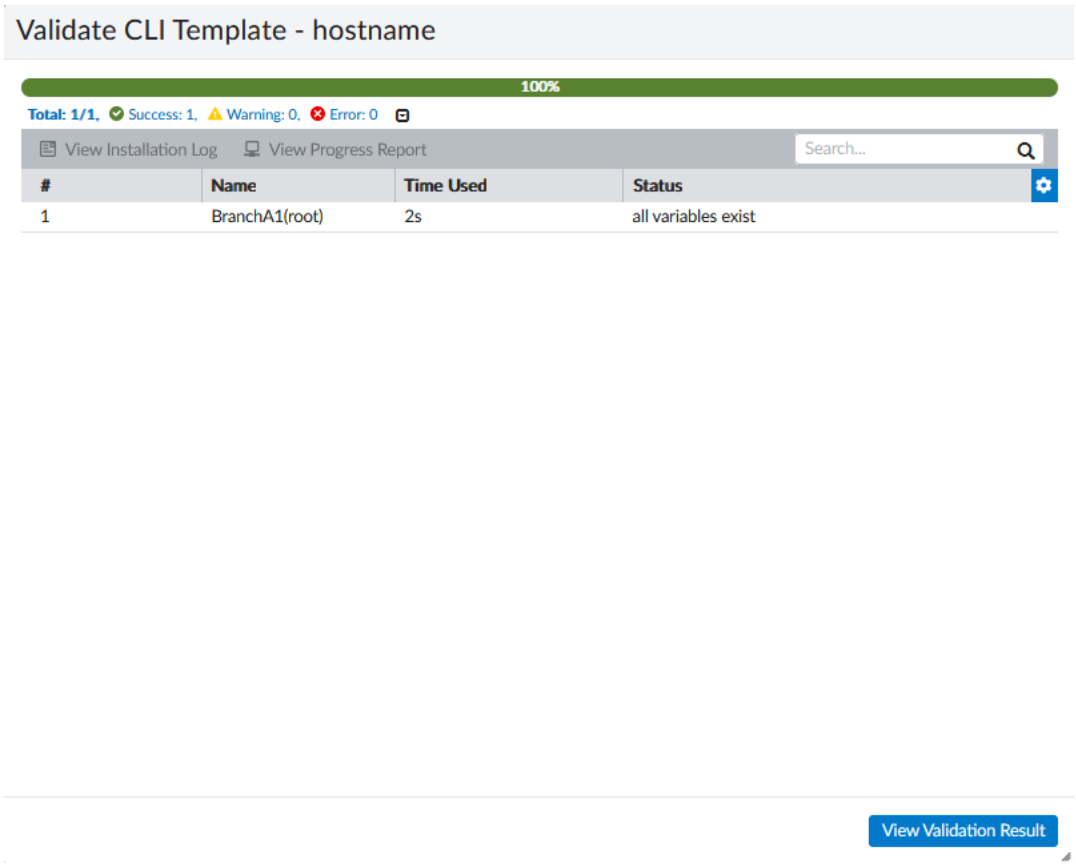
3. Once the template validation finishes, detected errors are displayed, and you can check the error for details. For example, variables missed.



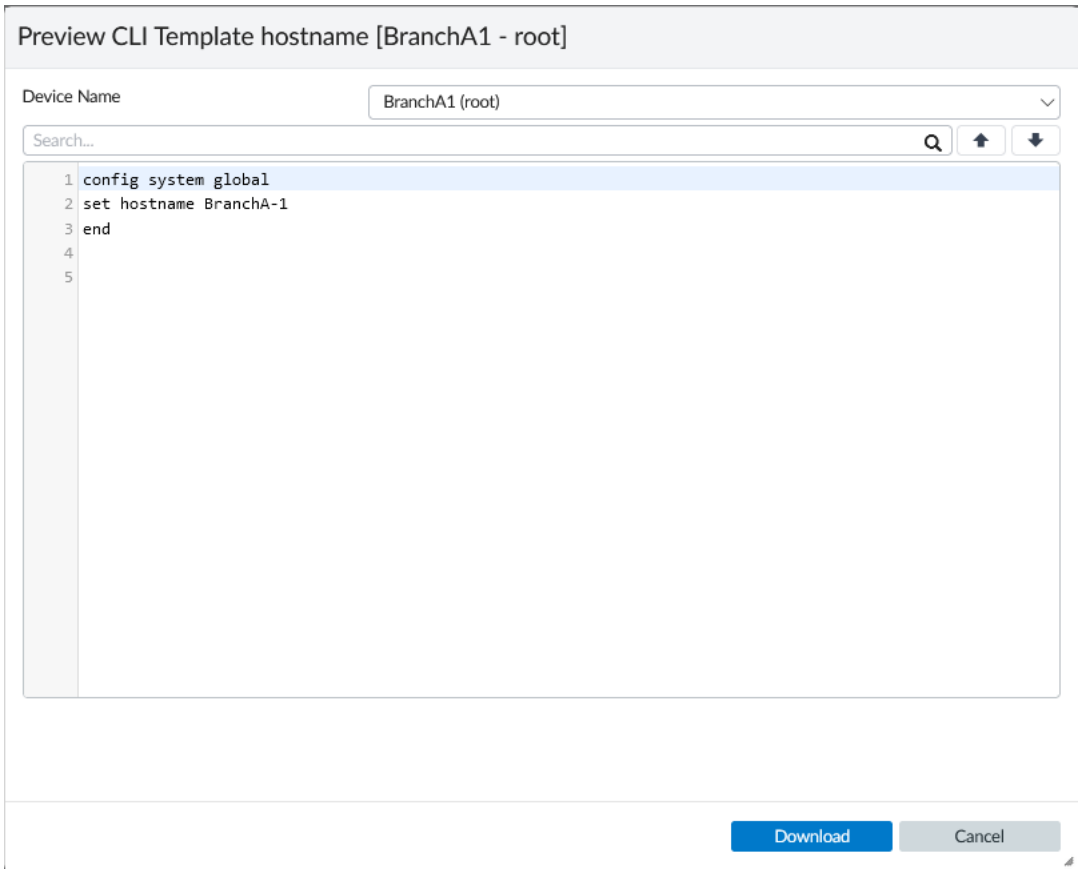
4. Click *View Validation Result*. In the *Validation Results* dialog, you can input the value for the missing variable.




5. When the CLI template passes validation, you can preview the script by clicking the *View Validation Result*.



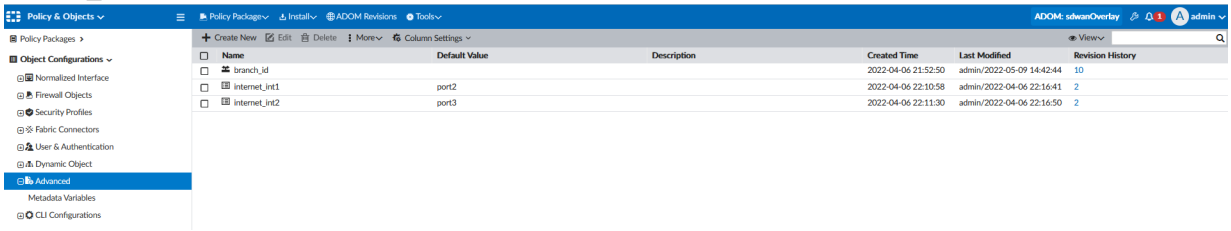

In the *Validation Result* dialog, click *Preview Script*. You can review the script details in the *Preview CLI Template* dialog.




## Import/export metadata variables

**To export metadata variables into JSON files:**

1. Go to *Policy & Objects* > *Object Configurations* > *Metadata Variables*.
2. Select the *More* menu from the toolbar, and click *Export Metadata Variables*. All metadata variables in this ADOM will be exported into a JSON file.
   In this example, there are three metadata variables in the ADOM *sdwanOverlay*: *branch_id*, *internet_int1*, and *internet_int2*.




After exporting these metadata variables, the metadata_variable.json file includes the following content:

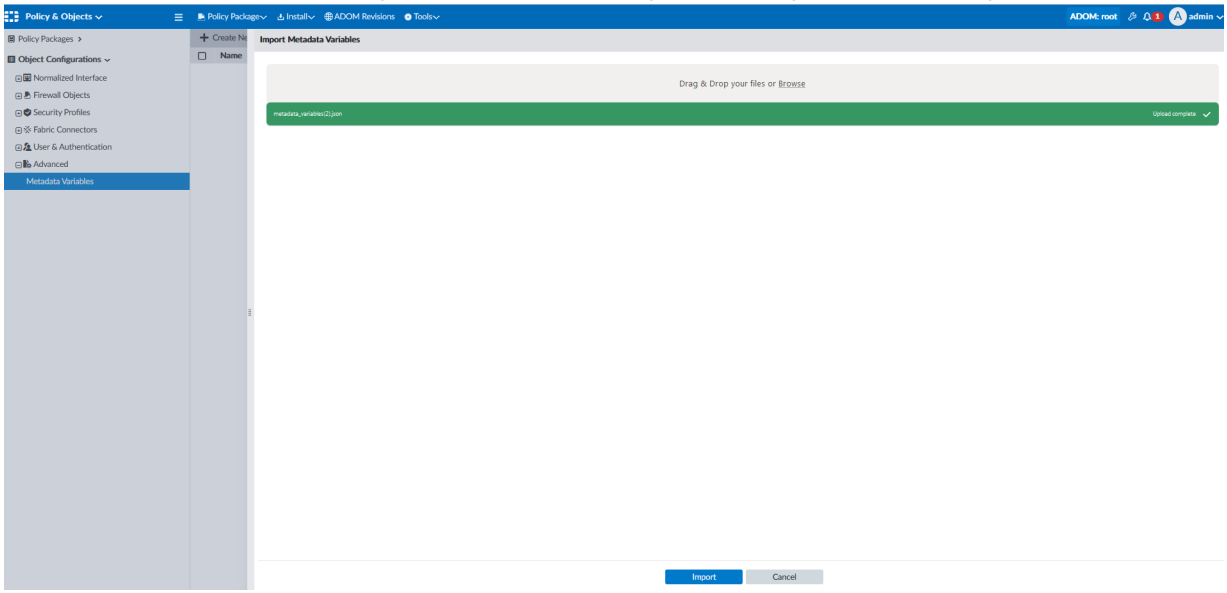
```
{
"adom": "sdwanOverlay",
"variables": [
{
"name": "branch_id",
"mapping": [
{
```

```
"device": "Branch1",
"vdom": "",
"value": "1"
},
{
"device": "Branch3",
"vdom": "",
"value": "3"
},
{
"device": "Branch4",
"vdom": "",
"value": "4"
},
{
"device": "Branch5",
"vdom": "",
"value": "5"
},
{
"device": "BranchA1",
"vdom": "",
"value": "1"
}
]
},
{
"name": "internet_int1",
"value": "port2"
},
{
"name": "internet_int2",
"value": "port3"
}
]
}
```


**To import metadata variables:**

1. Go to *Policy & Objects* > *Object Configurations* > *Metadata Variables*.
2. Select the *More* menu from the toolbar, and click *Import Metadata Variables*.

3. Browse and select the file to be imported. Wait for the file upload to complete, and click *Import*.

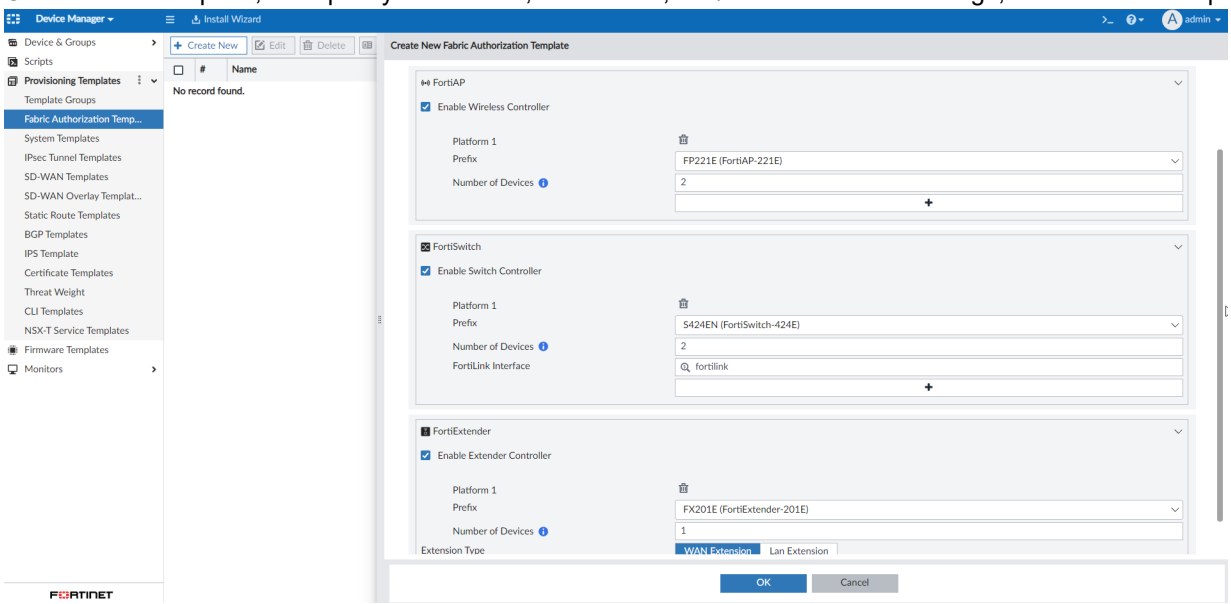



## Fabric Authorization Template automatically provisions and authorizes LAN Edge devices on the managed FortiGates - 7.2.1

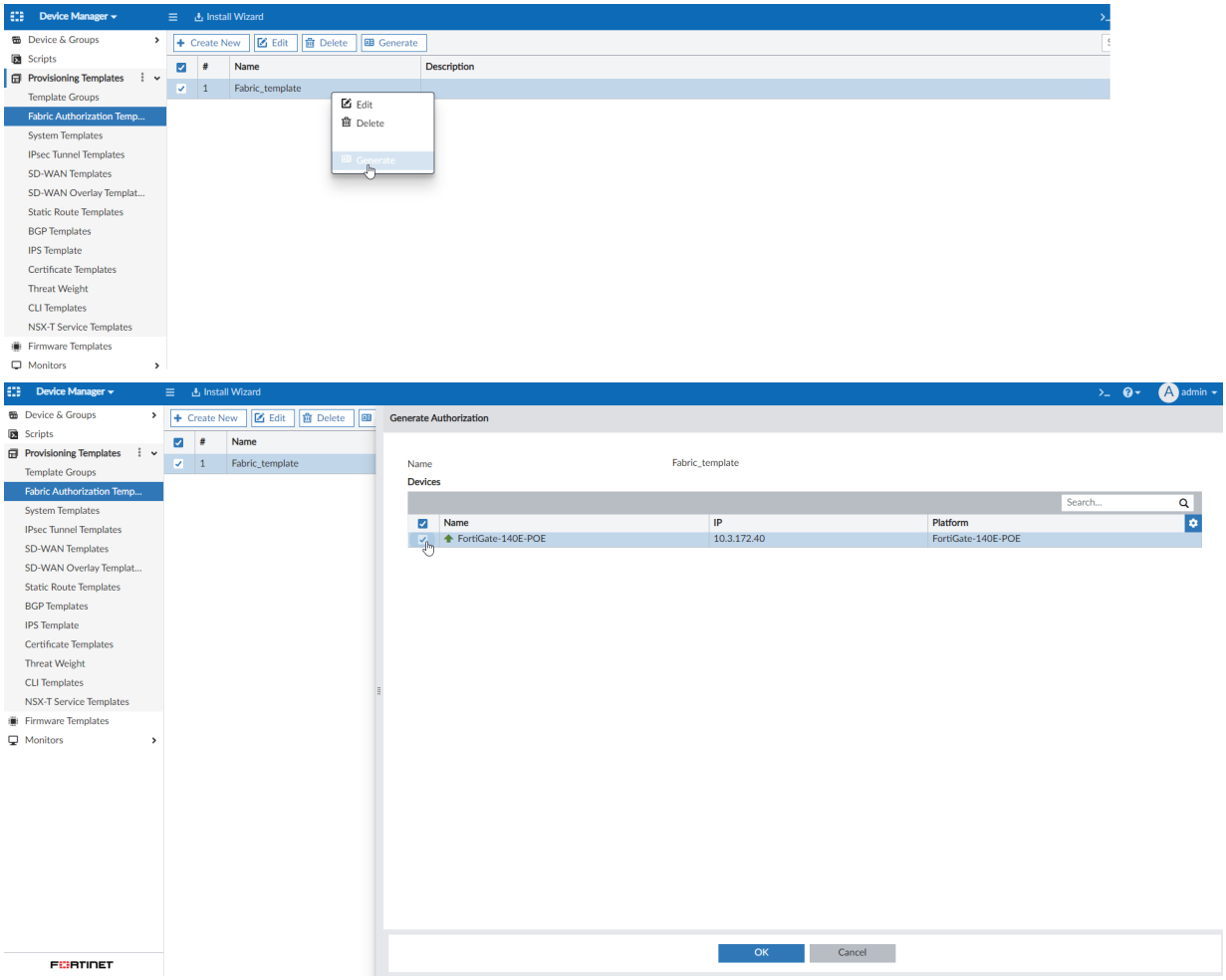
Fabric Authorization Template automatically provisions and authorizes LAN Edge devices on the managed FortiGates. Within the template we can enable the wireless and switch controllers and configure FortiLink interfaces.

**To configure the Fabric Authorization Template:**

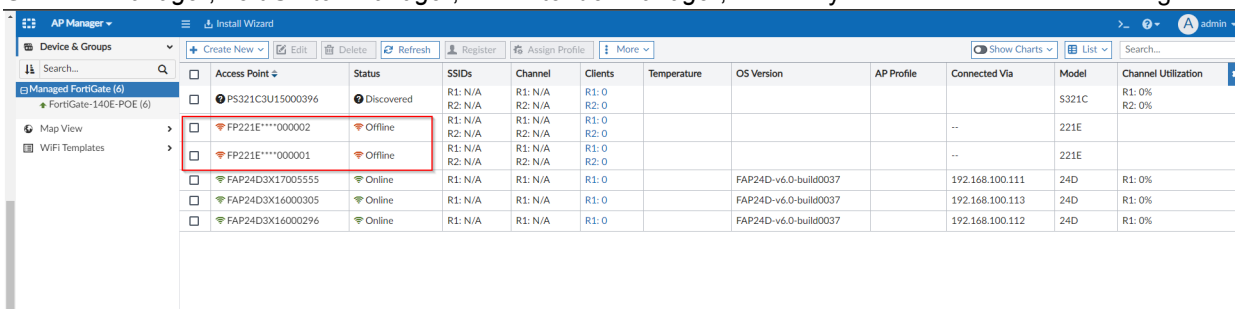
1. Go to *Device Manager* > *Provisioning Templates* > *Fabric Authorization Template*.
2. Create a new template, and specify the FortiAP, FortiSwitch, and/or FortiExtender settings, then save the template.

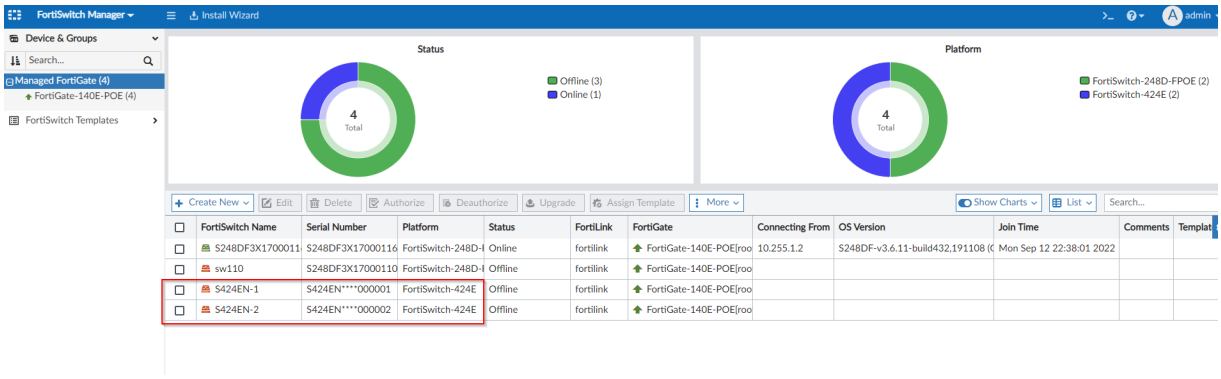


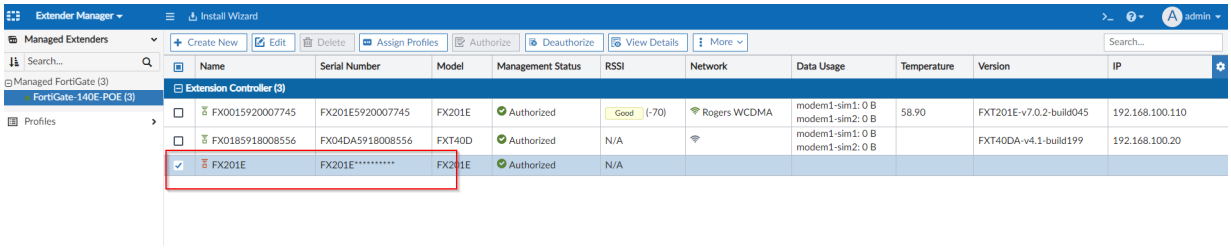
3. Right-click the template, and select Generate from the context menu, and then select the FortiGate to generate the wildcard entries.



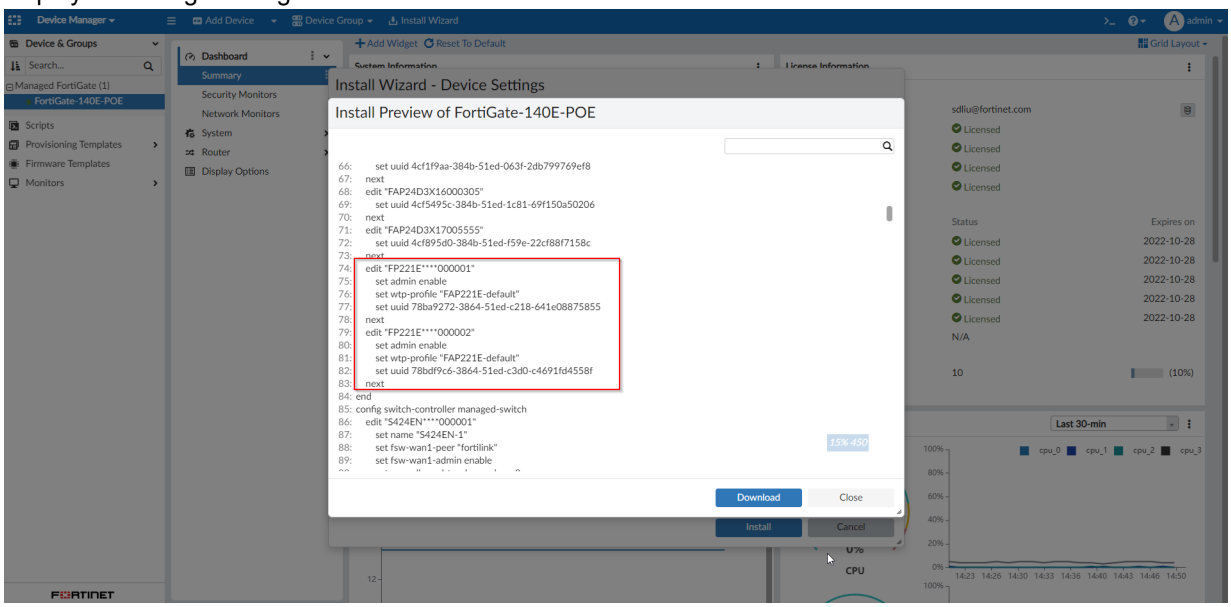

4. Go to *AP Manager*, *FortiSwitch Manager*, and *Extender Manager*, and verify that the wildcard entries are generated.






**5.** Deploy the changes using the Install Wizard.



# Central Management

This section lists the new features added to FortiManager for central management:



## AP Manager

This section lists the new features added to FortiManager for AP manager:



### AP Manager exposes wireless advanced features - 7.2.1

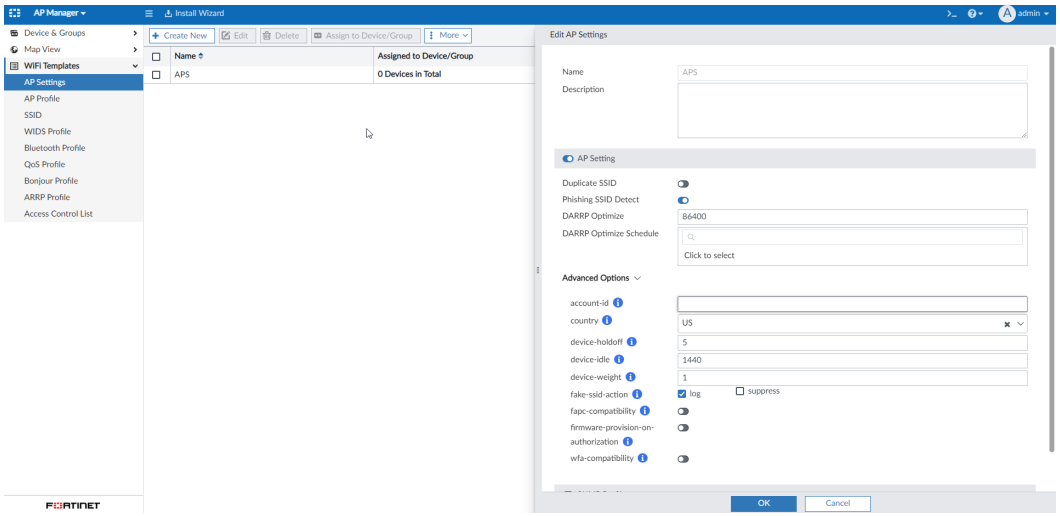
*AP Manager* exposes the wireless advanced features under the new *AP Settings*, *ARRP Profile*, and *Access Control List*.

This topic includes information about the following:

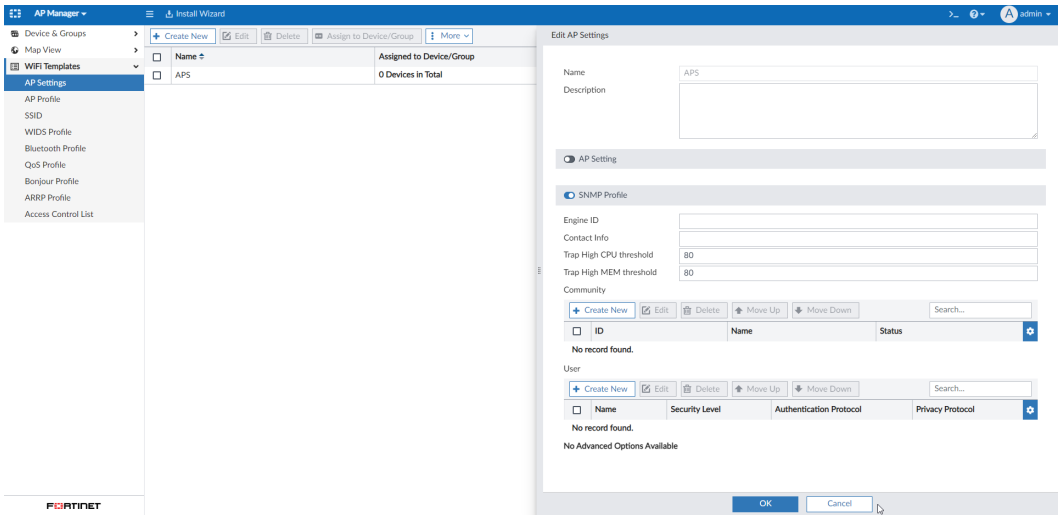
- AP Settings
- ARRP Profile
- Access Control List

**To use an AP Settings template:**

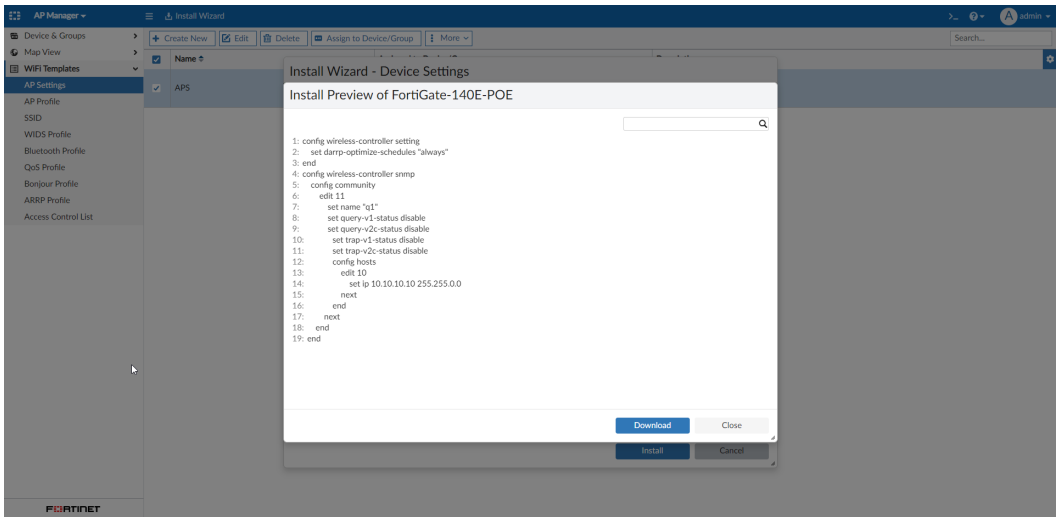
1. Go to *AP Manager* > *WiFi Templates* > *AP Settings*.
2. Click *Create New*, or edit an existing AP settings template.
3. Enable *AP Setting* to configure related options.
   You can expand *Advanced Options* to configure them as needed.




4. Enable *SNMP Profile* to configure related options.

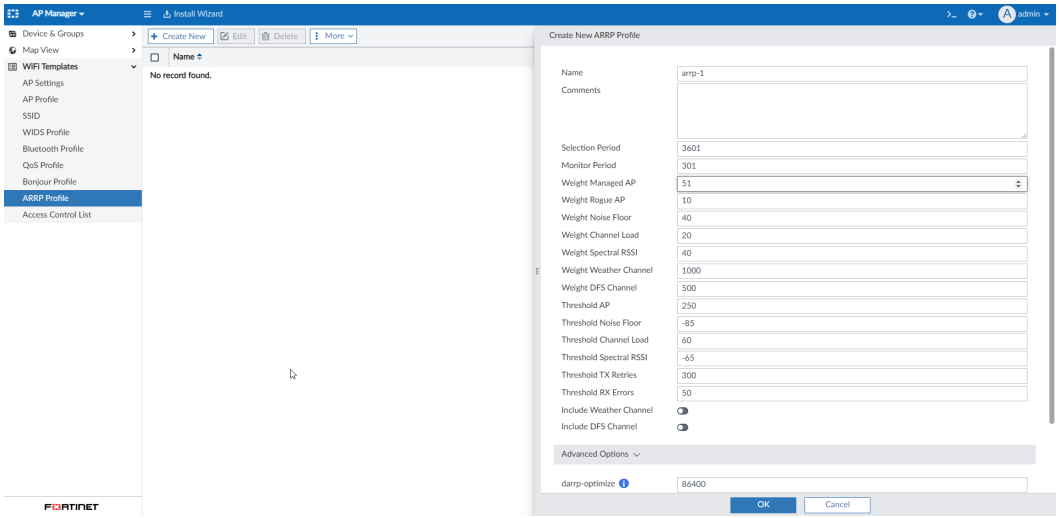



5. Click *OK*.
   The AP settings template can be assigned to a FortiGate device and then deployed using the *Install Wizard*. For example, see the install preview below.



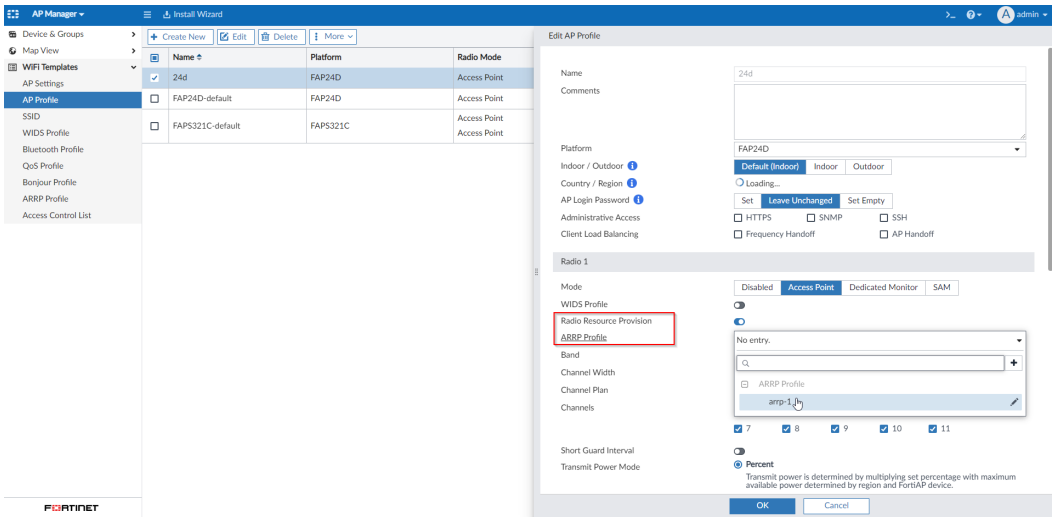

**To use an ARRP Profile:**

1. Go to *AP Manager* > *WiFi Templates* > *ARRP Profile*.
2. Click *Create New*, or edit an existing ARRP Profile.
3. Configure the ARRP Profile and click *OK*.

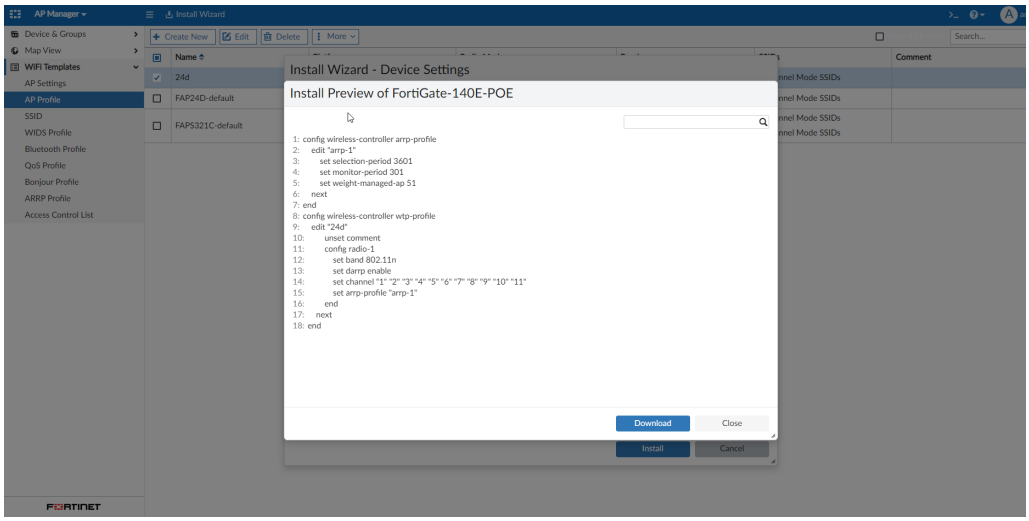



4. Go to *AP Manager* > *WiFi Templates* > *AP Profile*.
5. Click *Create New*, or edit an existing AP Profile.
6. Under the *Radio 1* settings, enable *Radio Resource Provision*.

7. From the *ARRP Profile* dropdown, select the ARRP profile.



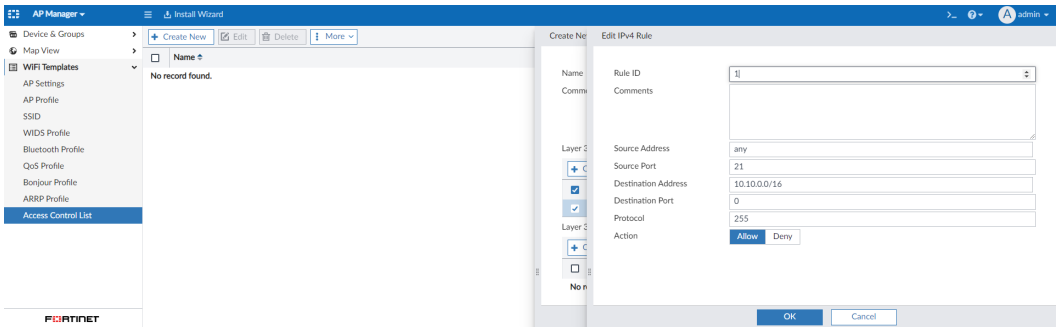

8. Configure the other options for the AP Profile, and click *OK*.
   The settings can be deployed to FortiGate when the AP profile is assigned to a FortiAP. For example, see the install preview below.



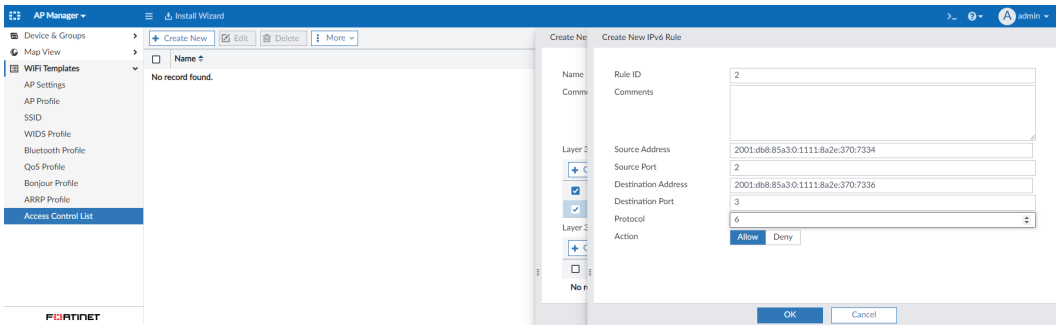

### To use an Access Control List:

1. Go to *AP Manager* > *WiFi Templates* > *Access Control List*.
2. Click *Create New*, or edit an existing Access Control List.

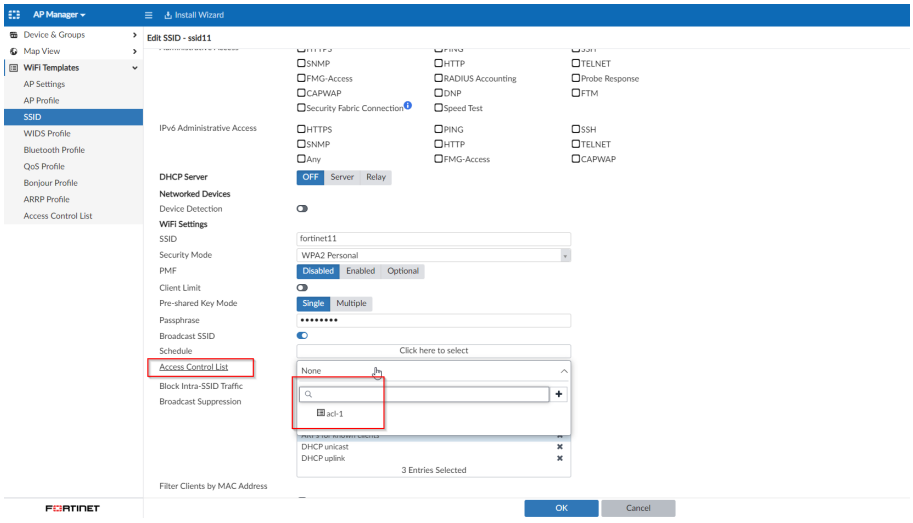
3. Create *Layer 3 IPv4 Rules* for the Access Control List.



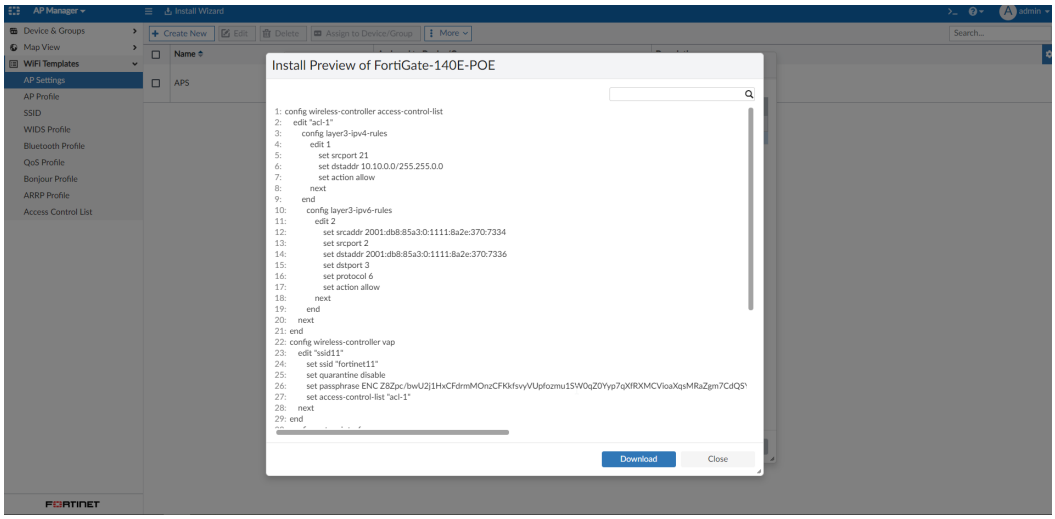

4. Create *Layer 3 IPv6 Rules* for the Access Control List.




5. Configure the other options for the Access Control List, and click *OK*.
6. Go to *AP Manager* > *WiFi Templates* > *SSID*.
7. Click *Create New*, or edit an existing SSID.
8. Go to the *WiFi Settings* section.
9. From the *Access Control List* dropdown, select the Access Control List.




10. Configure the other options for the SSID, and click *OK*.
    The settings can be deployed to FortiGate when the SSID is assigned to a FortiAP. For example, see the install preview below.




# FortiSwitch Manager

This section lists the new features added to FortiManager for FortiSwitch manager:

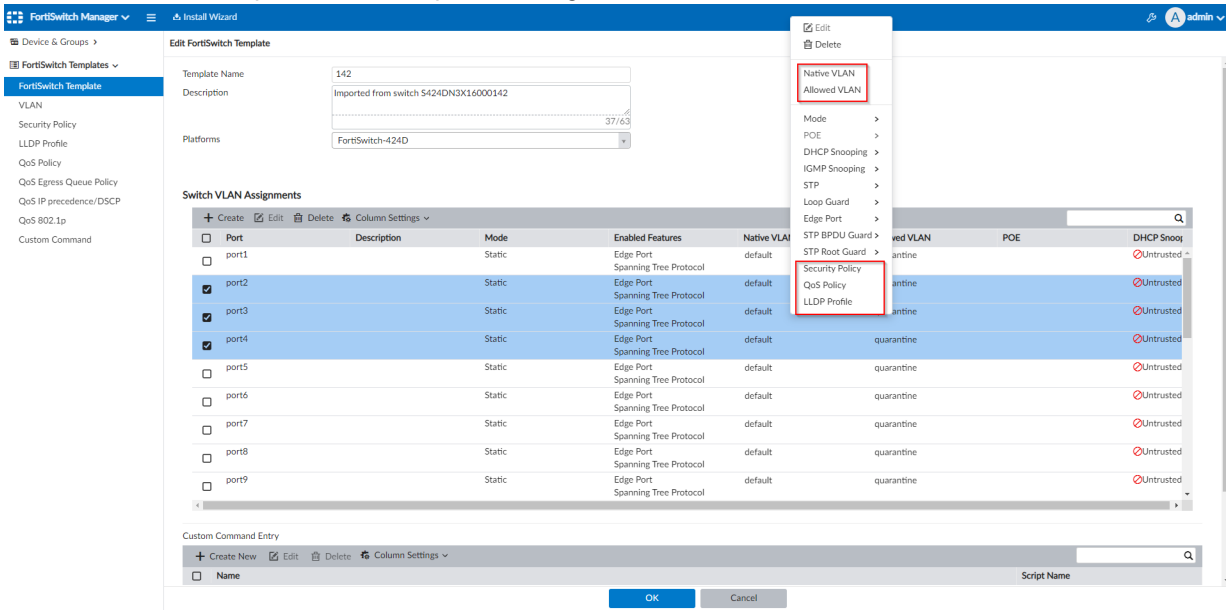


## Configuration enhancement improves multiple port selection in FortiSwitch Templates

In FortiManager 7.2.0, a configuration enhnacement improves multiple port selection in FortiSwitch Templates to optimize the admin workflow.

### To view FortiSwitch multi-port selection enhancements:

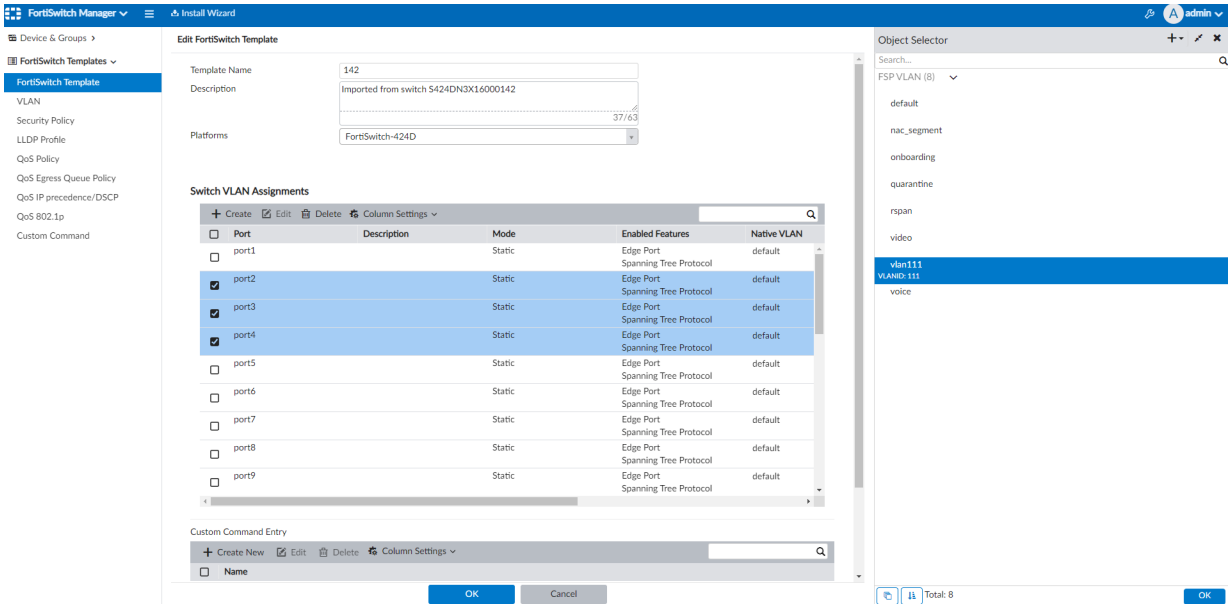
1. In FortiManager, go to *FortiSwitch Manager* > *FortiSwitch Templates*.
2. Edit a FortiSwitch Template, select the ports, and right-click to see the context menu.

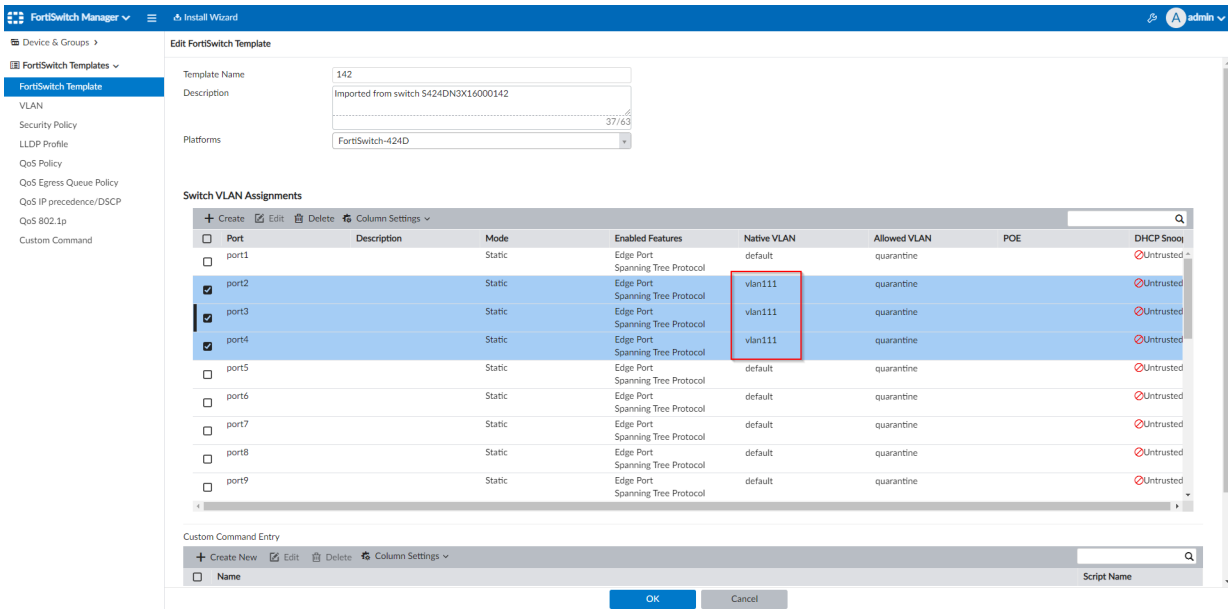



The following options are now available in the dropdown menu.

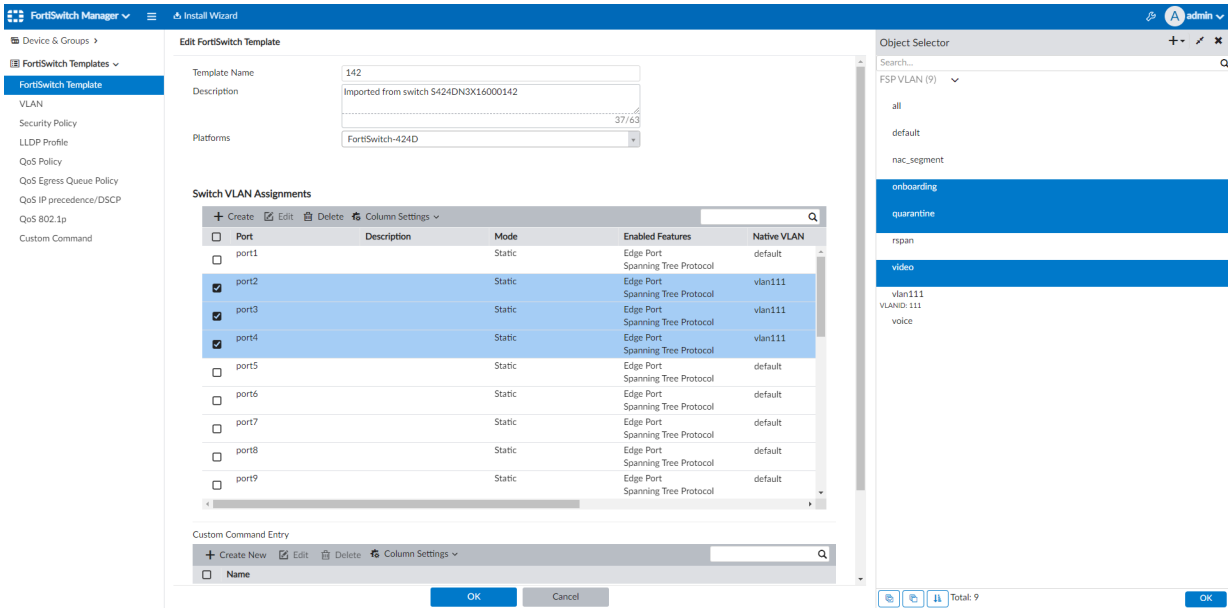
- Native VLAN
- Allowed VLAN
- Security Policy
- QoS Policy
- LLDP Profile

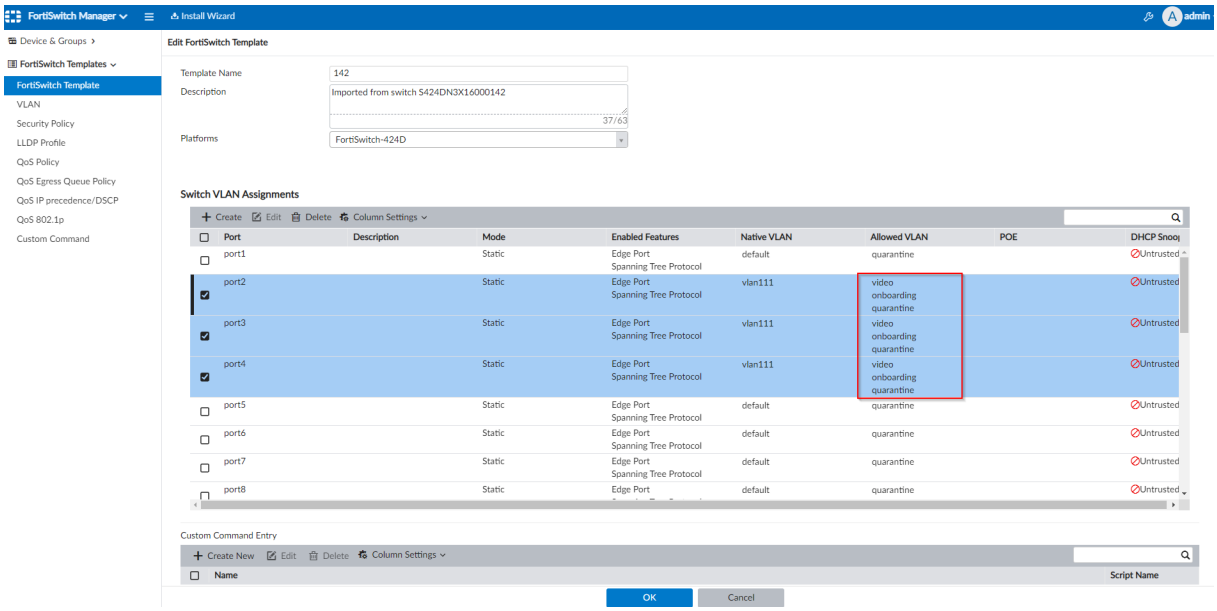
As an example, if you choose *Native VLAN*, you can select the native VLAN from the object selector.






As another example, when choosing *Allowed VLAN*, you can use the object selector to set the allowed VLAN.






3. After the settings are applied, you can install the changes to a FortiGate.

## NAC policy added to policy package - 7.2.1

The network access control (NAC) policy is added to manage policies for FortiSwitches in per-device or central management mode.

You can create a NAC policy that matches devices with the specified criteria, devices belonging to a specified user group, or devices with a specified FortiClient EMS tag. Devices that match the policy are assigned to a specific VLAN or have port-specific settings applied to them.

*FortiSwitch Manager* also supports dynamic port policy and FortiLink configuration.

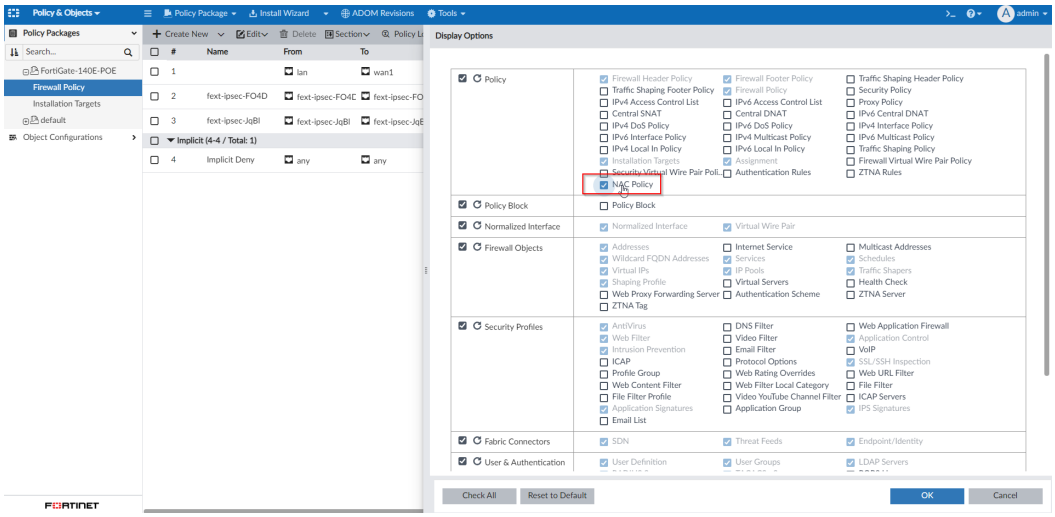
This topic includes steps to create:

- a NAC Policy
- a dynamic firewall address
- a dynamic port policy
- a FortiLink Settings template

**To create a NAC Policy:**

To make the *NAC Policy* option available, you must enable it in the *Display Options* for *Policy & Objects*.

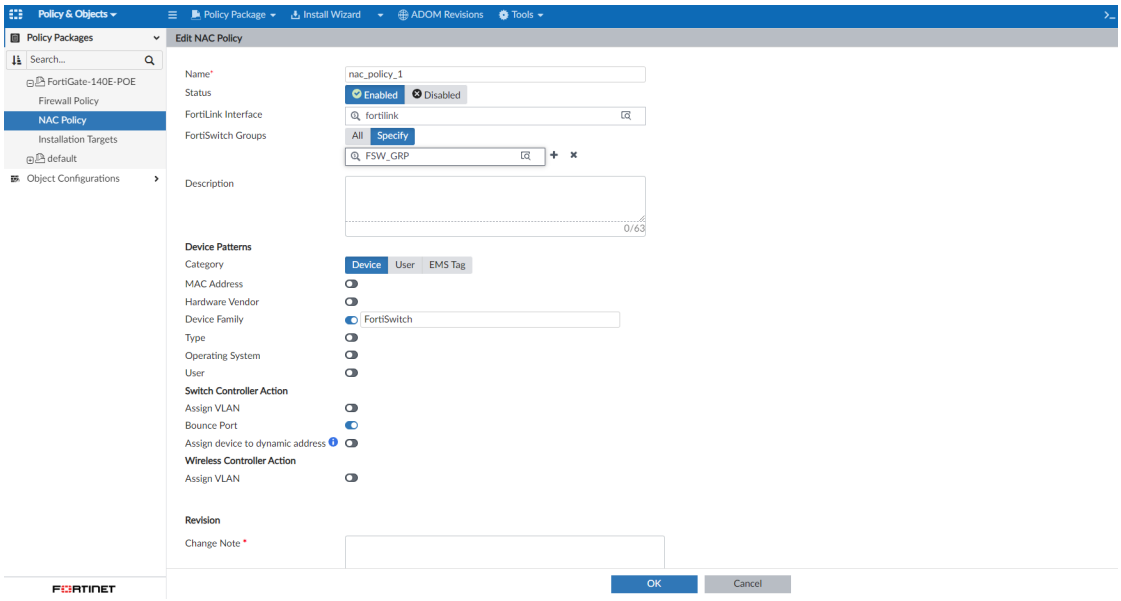
Go to *Policy & Objects* > *Tools* > *Display Options*. In the *Policy* section, select the checkbox for *NAC Policy* and click *OK*. The *NAC Policy* option will now display in the tree menu.



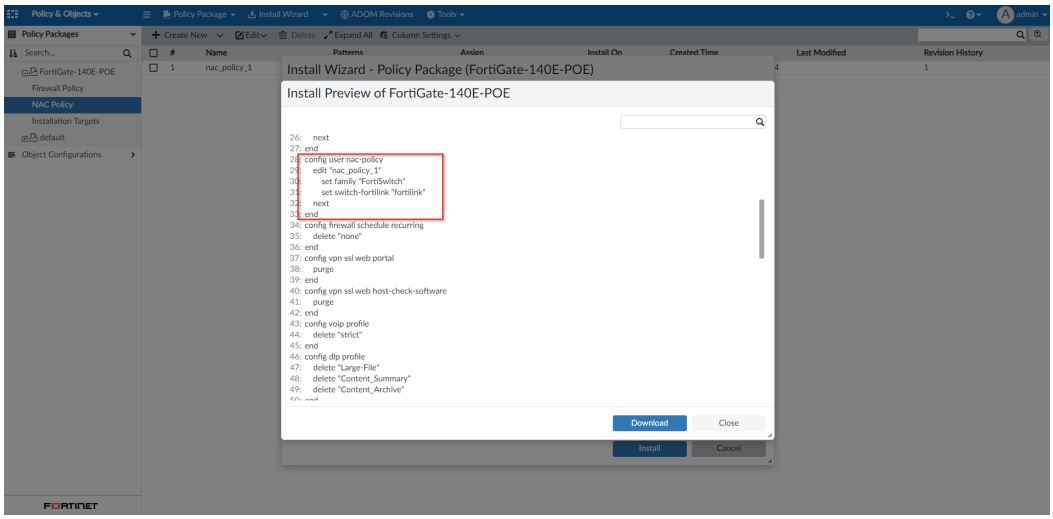

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the FortiGate policy package, select *NAC Policy*.
4. Click *Create New*.
5. Enter the following information:

| Option | Description |
|---|---|
| **Name** | Enter a unique name for the policy. |
| **Status** | Set the policy to *Enabled* or *Disabled*. |
| **FortiLink Interface** | Use the search field to find and select the FortiLink interface. |
| **FortiSwitch Groups** | Select *All* or *Specify* the FortiSwitch groups. |
| **Description** | Optionally, add a description for the policy. |
| **Device Patterns** | |
| **Category** | Select *Device*, *User*, or *EMS Tag*.<br>For *Device* pattern fields, you can use the wildcard * character when entering the value to be matched. |
| **MAC Address** | Enable or disable matching a MAC address, then enter a MAC address.<br>Only available if *Category* is *Device*. |
| **Hardware Vendor** | Enable or disable matching a hardware vendor, then enter a hardware vendor name.<br>Only available if *Category* is *Device*. |
| **Device Family** | Enable or disable matching a device family, then enter a device family name.<br>Only available if *Category* is *Device*. |
| **Type** | Enable or disable matching a device type, then enter a device type.<br>Only available if *Category* is *Device*. |

| Option | Description |
|---|---|
| **Operating System** | Enable or disable matching an operating system, then enter an operating system.<br>Only available if *Category* is *Device*. |
| **User group** | Select a user group.<br>Only available if *Category* is *User*. |
| **FortiClient EMS Tag** | Select a FortiClient EMS tag.<br>Only available if *Category* is *EMS Tag*. |
| **Switch Controller Action** | |
| **Assign VLAN** | Enable to select a VLAN interface for the switch controller action. |
| **Bounce Port** | Enable or disable the bounce port. |
| **Assign device to dynamic address** | Enable to use a dynamic firewall address for matching a device, then select the address. See To create a dynamic firewall address for the NAC Policy: on page 88 below. |
| **Wireless Controller Action** | |
| **Assign VLAN** | Enable to select a VLAN interface for the wireless controller action. |
| **Revision** | |
| **Change Note** | Add a description of the changes being made to the policy. This field is required. |

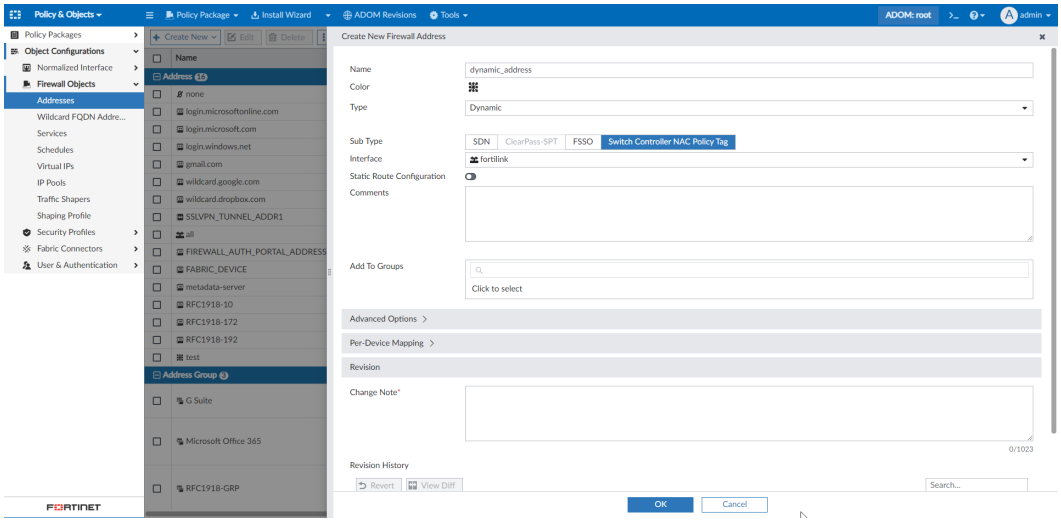



6. Click *OK* to save the policy.
   You can now deploy the NAC policy using the *Install Wizard*. For example, see the install preview below:

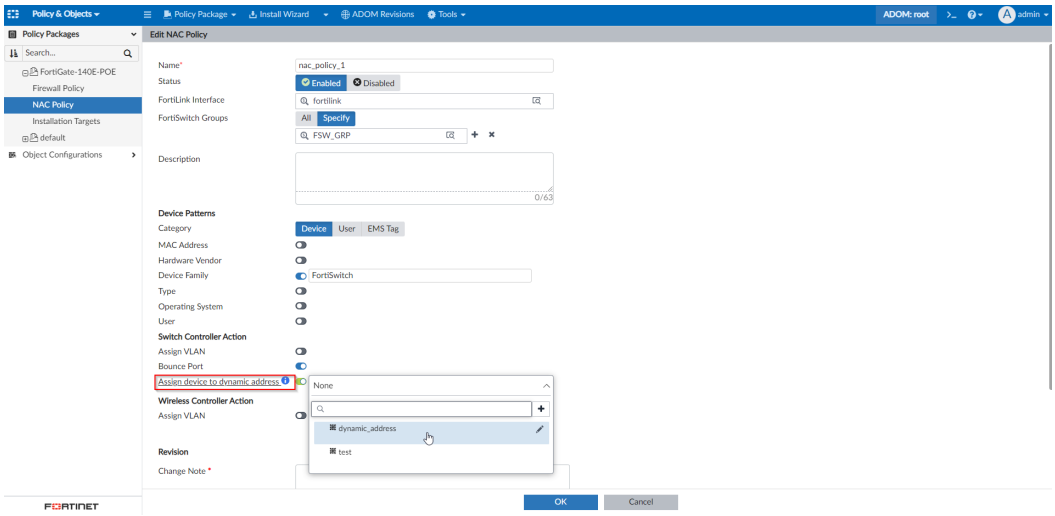



**To create a dynamic firewall address for the NAC Policy:**

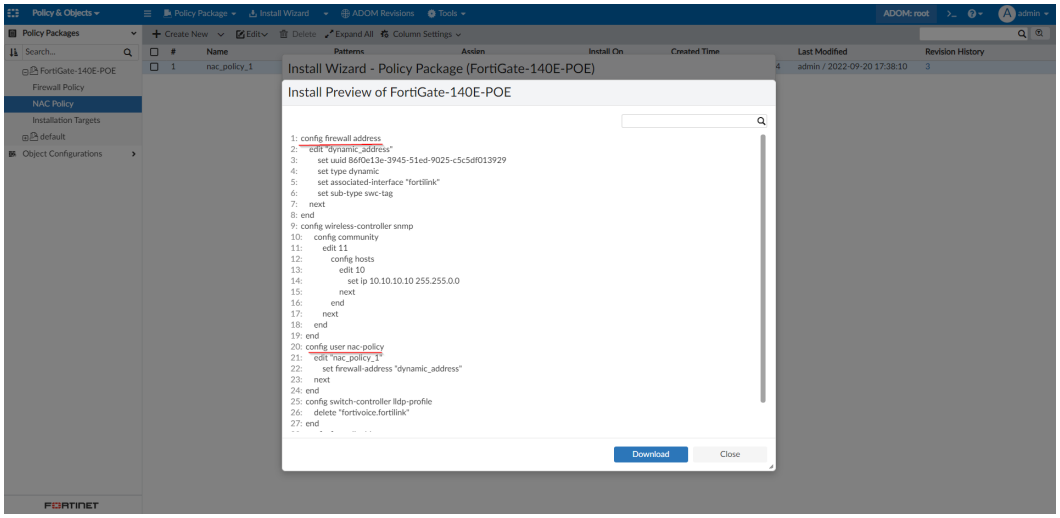
1. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Addresses*.
2. Click *Create New*.
3. From the *Type* dropdown, select *Dynamic*.
4. For the *Sub Type* field, select *Switch Controller NAC Policy Tag*.
5. From the *Interface* dropdown, select the FortiLink interface.
6. Configure the other options, as needed.




7. Click *OK* to save the dynamic firewall address.
   You can now use the dynamic firewall address in a NAC policy through the *Assign device to dynamic address* option. For example, see the NAC policy configuration below:




The firewall address will be included when the NAC policy is deployed. For example, see the install preview below:

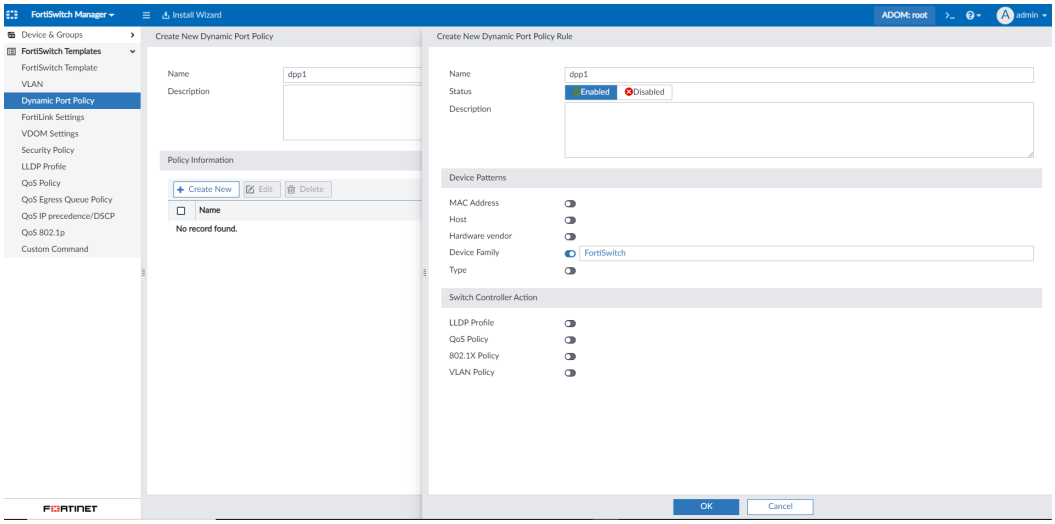



**To create a dynamic port policy:**

1. Go to *FortiSwitch Manager* > *FortiSwitch Templates* > *Dynamic Port Policy*.
2. Click *Create New*, and enter a *Name* for the dynamic port policy.
3. In the *Policy Information* section, click *Create New*.
4. Enter the following information for the dynamic port policy rule:

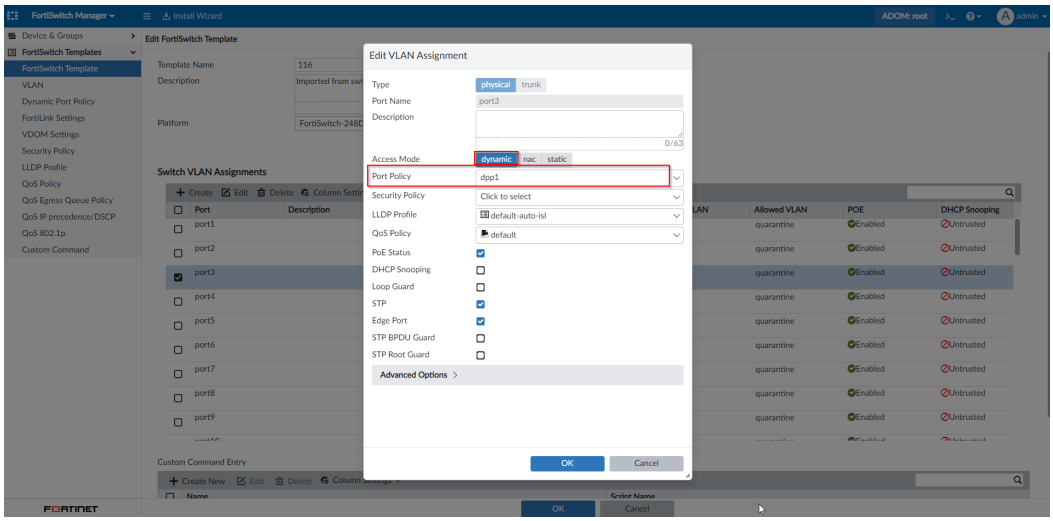
| Option | Description |
|---|---|
| **Name** | Enter a unique name for the dynamic port policy rule. |
| **Status** | Set the rule to Enabled or Disabled. |
| **Description** | Optionally, enter a description for the rule. |
| **Device Patterns** | |
| **MAC Address** | Enable or disable matching a MAC address, then enter a MAC address. |

| Option | Description |
|---|---|
| **Host** | Enable or disable matching a host address, then enter a host address. |
| **Hardware Vendor** | Enable or disable matching a hardware vendor, then enter a hardware vendor name. |
| **Device Family** | Enable or disable matching a device family, then enter a device family name. |
| **Type** | Enable or disable matching a device type, then enter a device type. |
| **Switch Controller Action** | |
| **LLDP Profile** | Enable to select an LLDP profile for the switch controller action. |
| **QoS Policy** | Enable to select a QoS policy for the switch controller action. |
| **802.1X Policy** | Enable to select an 802.1X policy for the switch controller action. |
| **VLAN Policy** | Enable to select a QoS policy for the switch controller action. |

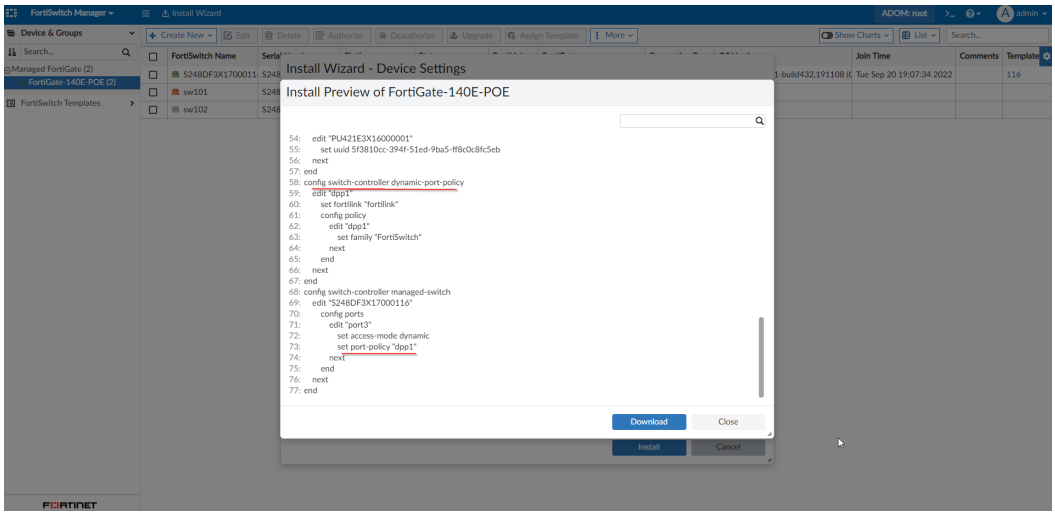



5. Click *OK* to save the dynamic port policy.
6. Go to *FortiSwitch Manager* > *FortiSwitch Templates* > *FortiSwitch Template*.
7. Click *Create New*, and enter a *Template Name* and *Platform*.
8. In the *Switch VLAN Assignments* table, select a port and click *Edit*.
   The *Edit VLAN Assignment* dialog displays.
9. For the *Access Mode* field, select *dynamic*.

10. From the *Port Policy* dropdown, select the dynamic port policy.




11. Click *OK*.
12. Click *OK* to save the FortiSwitch Template.
    The configuration will be deployed to the FortiGate device when the template is assigned to a FortiSwitch. For example, see the install preview below:

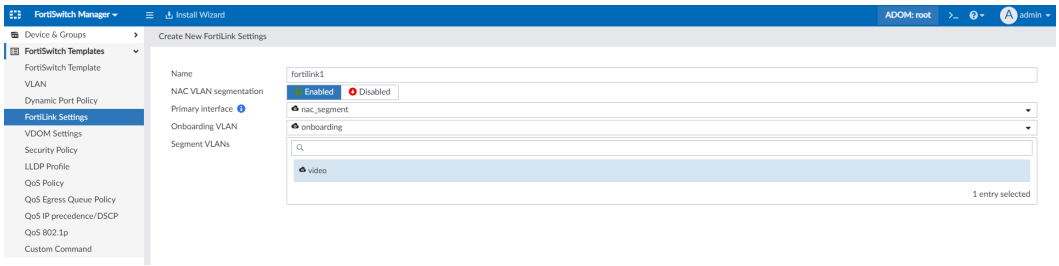



### To create a FortiLink Settings template:

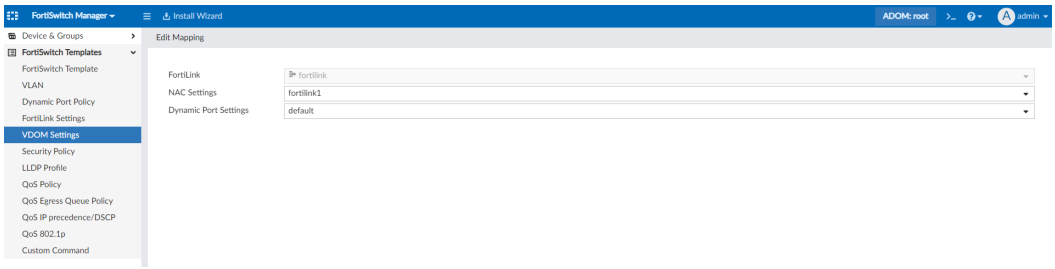
1. Go to *FortiSwitch Manager* > *FortiSwitch Templates* > *FortiLink Settings*.
2. Click *Create New*.
3. Enter the following information:

| Option | Description |
|---|---|
| **Name** | Enter a name for the FortiLink Settings template. |
| **NAC VLAN segmentation** | Enable or disable NAC VLAN segmentation. |
| **Primary Interface** | Select the primary interface. |

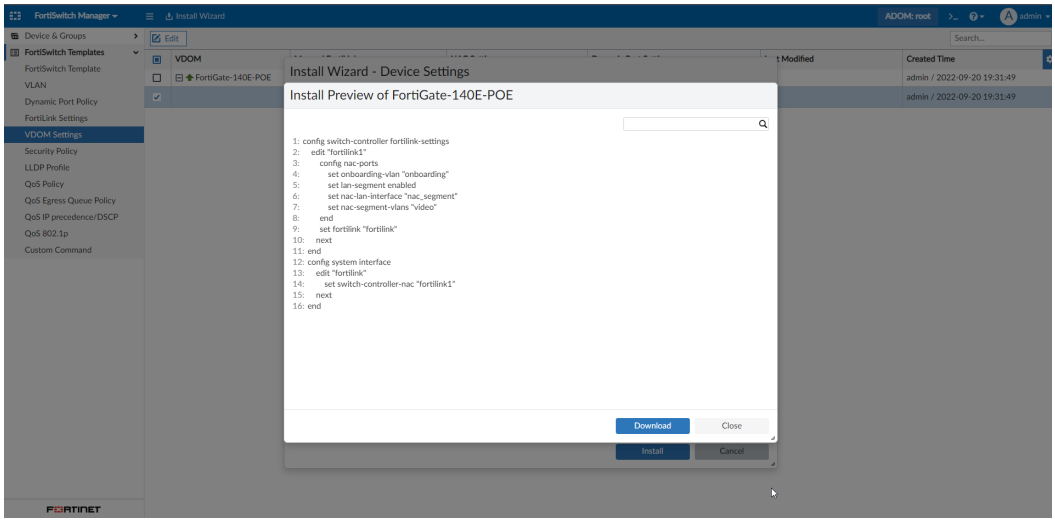
| Option | Description |
|---|---|
| **Onboarding VLAN** | Select the onboarding VLAN interface. |
| **Segment VLANs** | Select the segment VLANs. |




4. Click *OK* to save the FortiLink Settings template.
5. Go to *FortiSwitch Manager* > *FortiSwitch Templates* > *VDOM Settings*, and edit a FortiGate's mapped FortiLink.
6. From the *NAC Settings* dropdown, select the FortiLink settings template.




7. Click *OK*.
   The configuration can now be deployed to FortiGate devices, as needed. For example, see the install preview below:

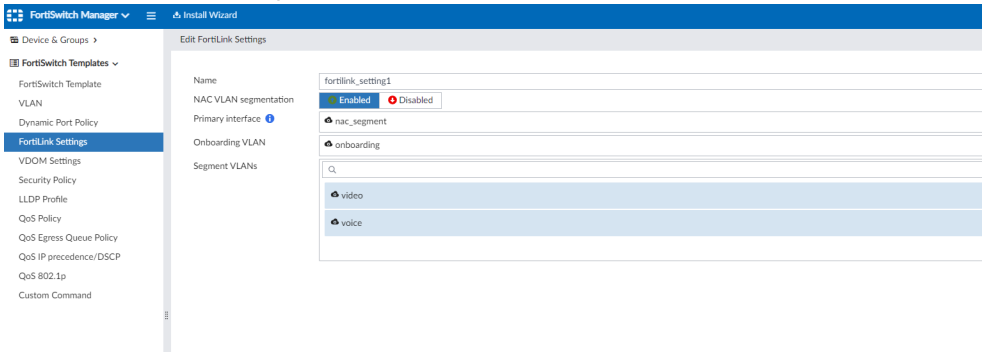


## NAC policy enhanced with FortiLink settings, LAN segments, and NAC policy tags - 7.2.1

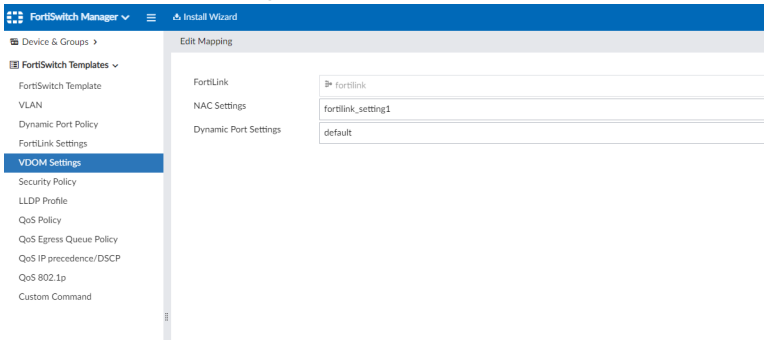
In FortiManager 7.2.1, NAC policies are enhanced with FortiLink settings (with VDOM support), LAN Segments, and NAC policy tags.

**To create a new FortiLink Setting template:**

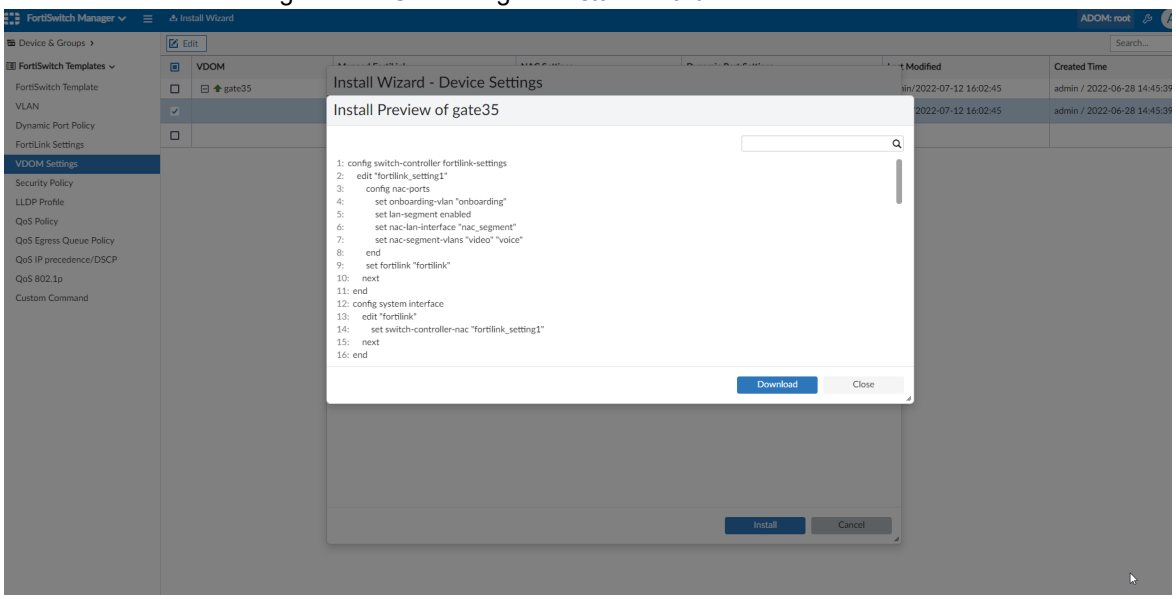
1. Go to *FortiSwitch Manager* > *FortiSwitch Templates* > *FortiLink Settings*, and click *Create New*.
2. Configure the details of the *FortiLink Settings* template, including the *Name*, *NAC VLAN Segmentation*, *Primary Interface*, *Onboarding VLAN*, and *Segment VLANs*.
3. Click *OK* to save the template.




4. Go to *FortiSwitch Manager* > *FortiSwitch Templates* > *VDOM Settings* to assign the FortiLink Settings template to a FortiGate in *NAC Settings*.

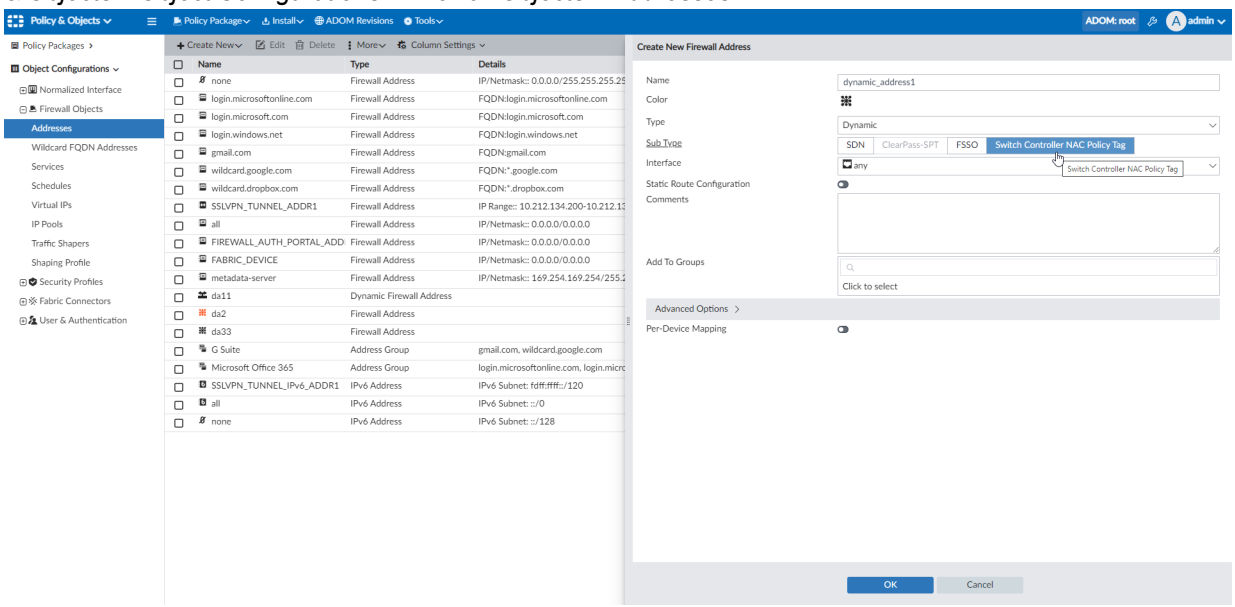


5. Install the FortiLink settings to FortiGate using the *Install Wizard*.

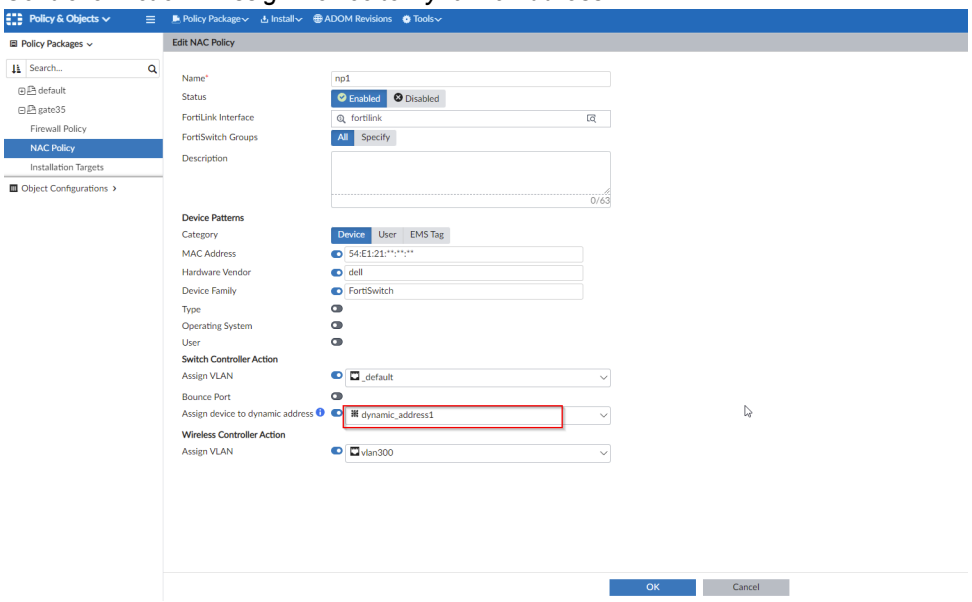



**To configure NAC policy tags:**

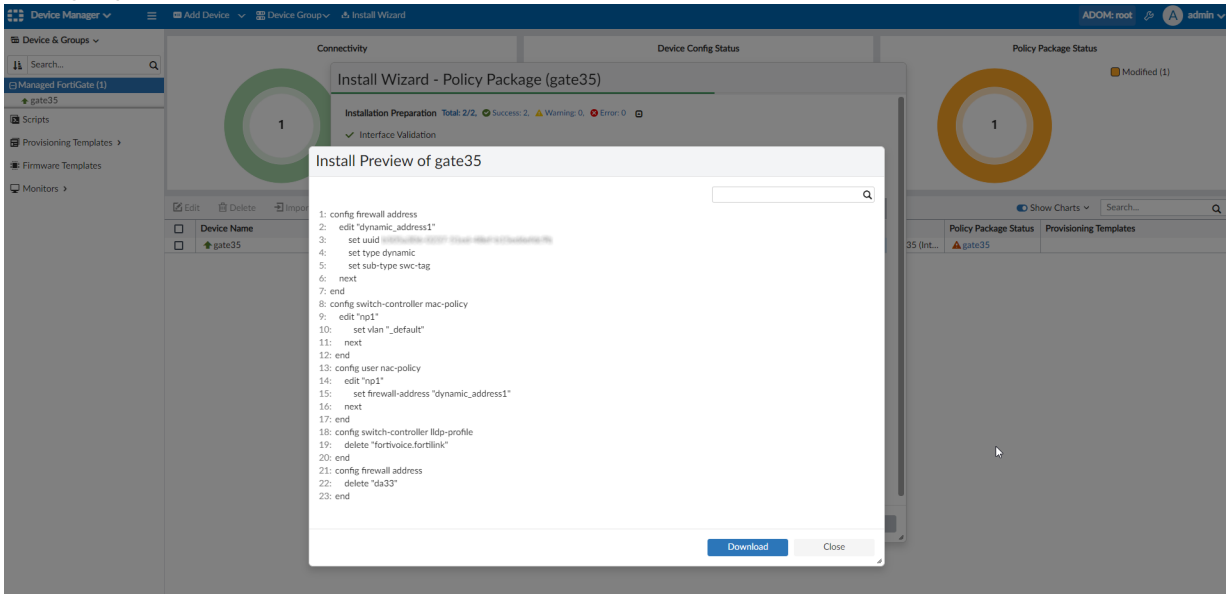
1. Dynamic Firewall Address with the *Switch Controller NAC Policy Tag Sub Type* can be created or edited in *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Addresses*.



2. The configured firewall address can be used in *Policy & Objects* > *Policy Packages* > *NAC Policy* > *Switch Controller Action* > *Assign Device to Dynamic Address*.



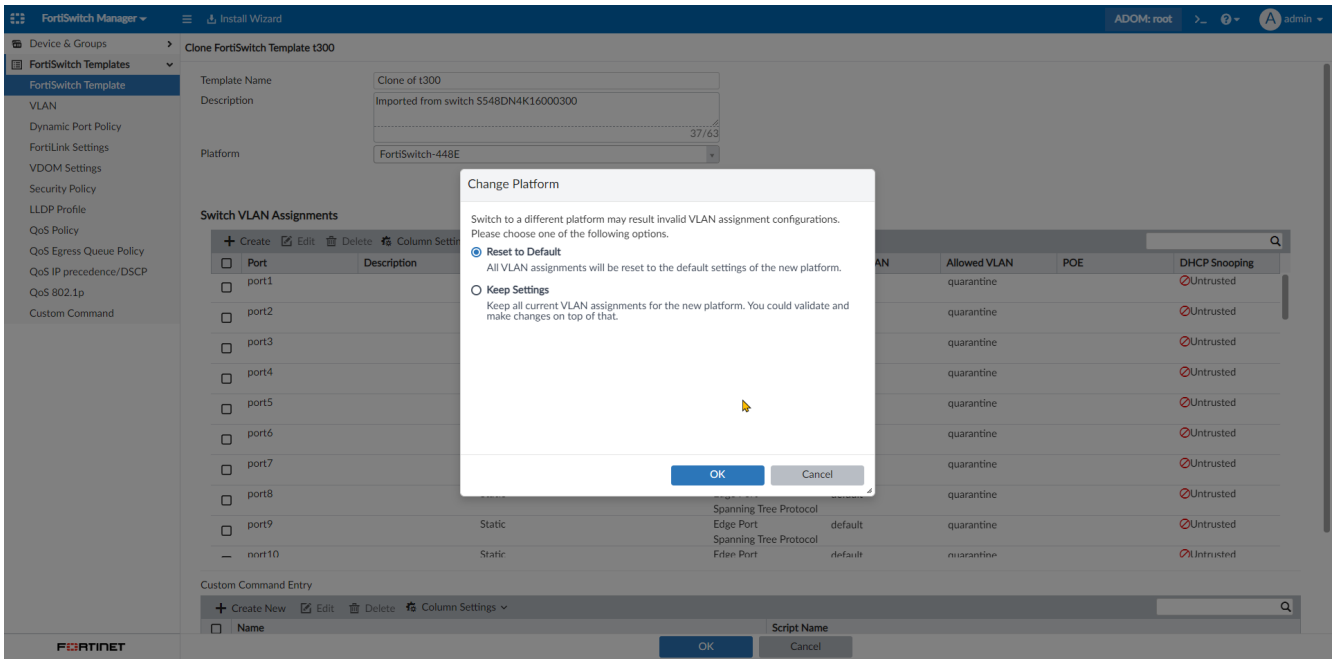

3. The NAC policy change can be installed to FortiGate using the Install Wizard's *Install Policy Packages & Device Settings* option.




## LAN-Edge: Keep VLAN info when cloning FortiSwitch template - 7.2.1

Cloning the FortiSwitch template to a a different switch platform can keep the VLAN settings from the source template.

If the switch model is changed, choose *Reset to Default* or *Keep Settings* when changing the FortiSwitch platform.




If *Reset to Default* is selected, the port configurations are discarded.

If *Keep Settings* is selected, the port configuration from the source template is copied into the cloned template.

- When the cloned template has more ports than the original, the additional ports do not appear in the template. You will have to add these ports manually.
- When the cloned template has fewer ports than the original, the additional ports must be deleted before you can save the cloned template.

# Extender Manager

This section lists the new features added to FortiManager for Extender manager:

- Extender Manager displays the ESN IMEI, phone number, IMSI, and ICCID as columns for all managed FortiExtenders 7.2.2 on page 96

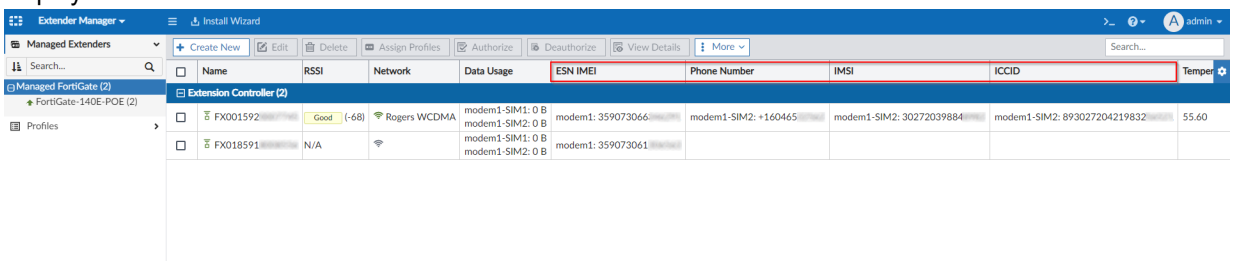
## Extender Manager displays the ESN IMEI, phone number, IMSI, and ICCID as columns for all managed FortiExtenders - 7.2.2

Extender Manager displays the ESN IMEI, phone number, IMSI, and ICCID as columns for all managed FortiExtenders.

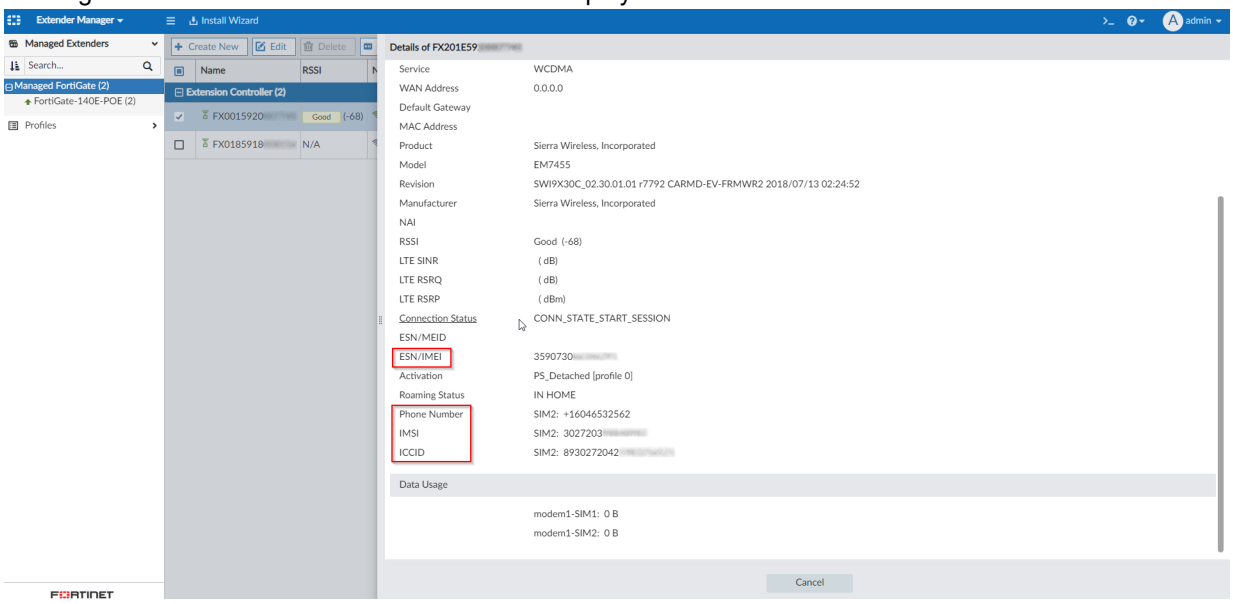
**To view the additional information for a FortiExtender:**

1. In FortiManager, go to *Extender Manager* > *Managed Extenders*.

2. The columns for ESN IMEI, Phone Number, IMSI, and ICCID are available and the relevant information is displayed.




3. Viewing the details of a FortiExtender device also displays this same information.




# Others

This section lists the new features added to FortiManager for other topics relating to central management:

## ADOM-level meta variables for general use in scripts, templates, and model devices

In FortiManager, ADOM-level meta variables are available for general use in scripts, templates, and model devices.

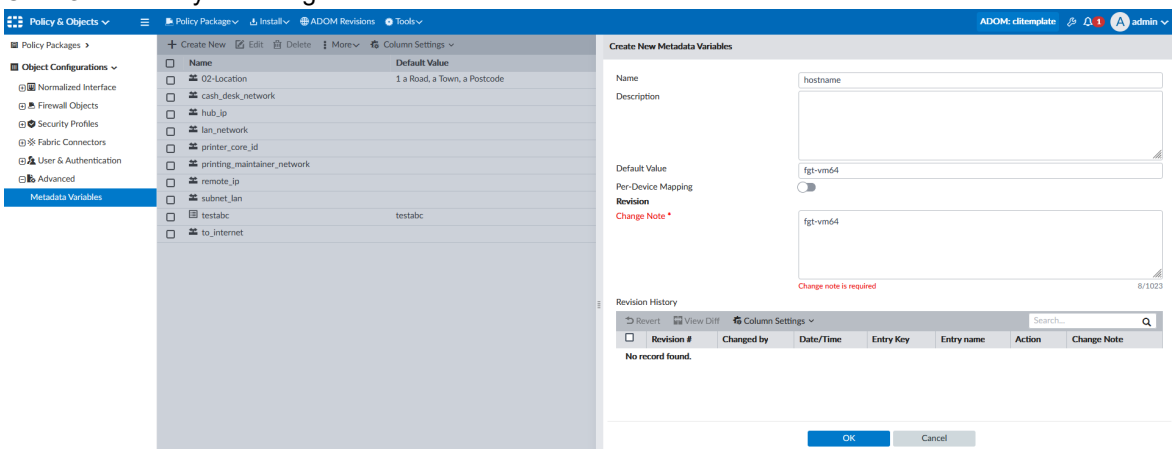
**To create and use an ADOM-level metadata variable:**

1. In FortiManager, enter the ADOM where the metadata variable will be used.
2. Enable the metadata variable object type in *Policy & Objects*.
   a. Go to *Policy & Objects*, click *Tools* in the toolbar, and select *Display Options*.
   b. Enable the *Metadata Variables* object under the *Advanced* category, and click *OK*.

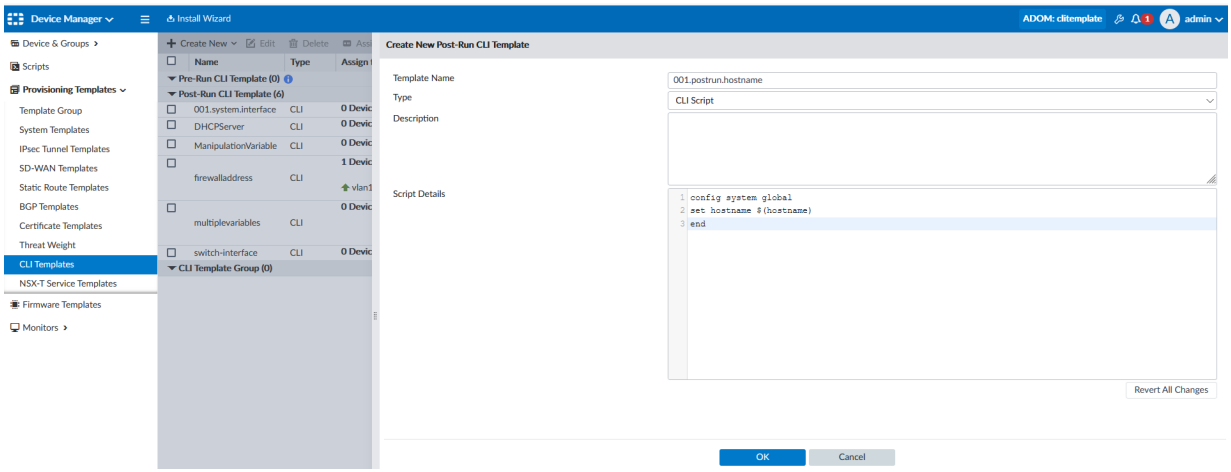
   In FortiManager 7.2.2 and later, *Display Options* has been renamed to *Feature Visibility*.
3. Create the metadata variable object.
   a. In *Policy & Objects*, go to *Object Configurations* > *Advanced* > *Metadata Variables*, and click *Create New*. The *Create New Metadata Variables* wizard opens.
   b. Enter the required information to create the metadata variable.
   In this example, the following metadata information is used:
   - *Name*: hostname
   - *Default Value*: fgt-vm64
   - *Per-Device Mapping*: ON

- Click *OK* to save your changes.



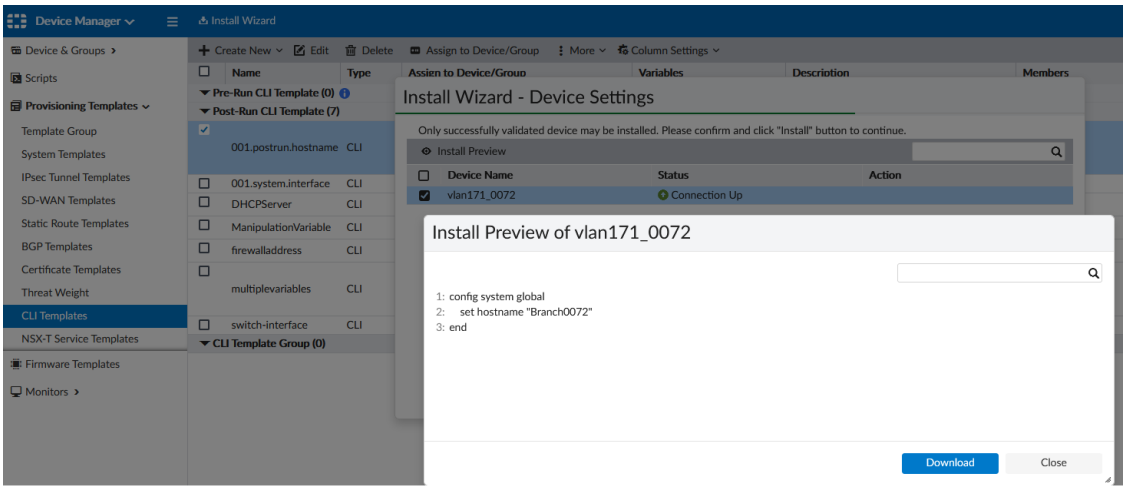

4. Create a CLI template that includes the metadata variable.
   a. Go to *Device Manager* > *Provisioning Templates* > *CLI Templates*, and click *Create New* > *Post-Run CLI Template*.
   The *Create Post-Run CLI Template* wizard opens.
   b. Enter the script details, including the metavariable, and click *OK*.
   In this example, the following CLI is used that includes the hostname metadata variable:

```
config system global
set hostname $(hostname)
end
```




5. Install the CLI template to a device.
   a. Go to *Device Manager* and assign the template to a model device or an online FortiGate device.
   b. Perform an installation using the *Install Wizard* to install device settings.
   In this example, the CLI template is assigned and installed to FortiGate "vlan171_0072". When an installation is performed, the install preview shows that the variable (hostname) has been substituted as per its per-device

value "Branch0072".




## One FortiAnalyzer can be shared across multiple FortiManager ADOMs

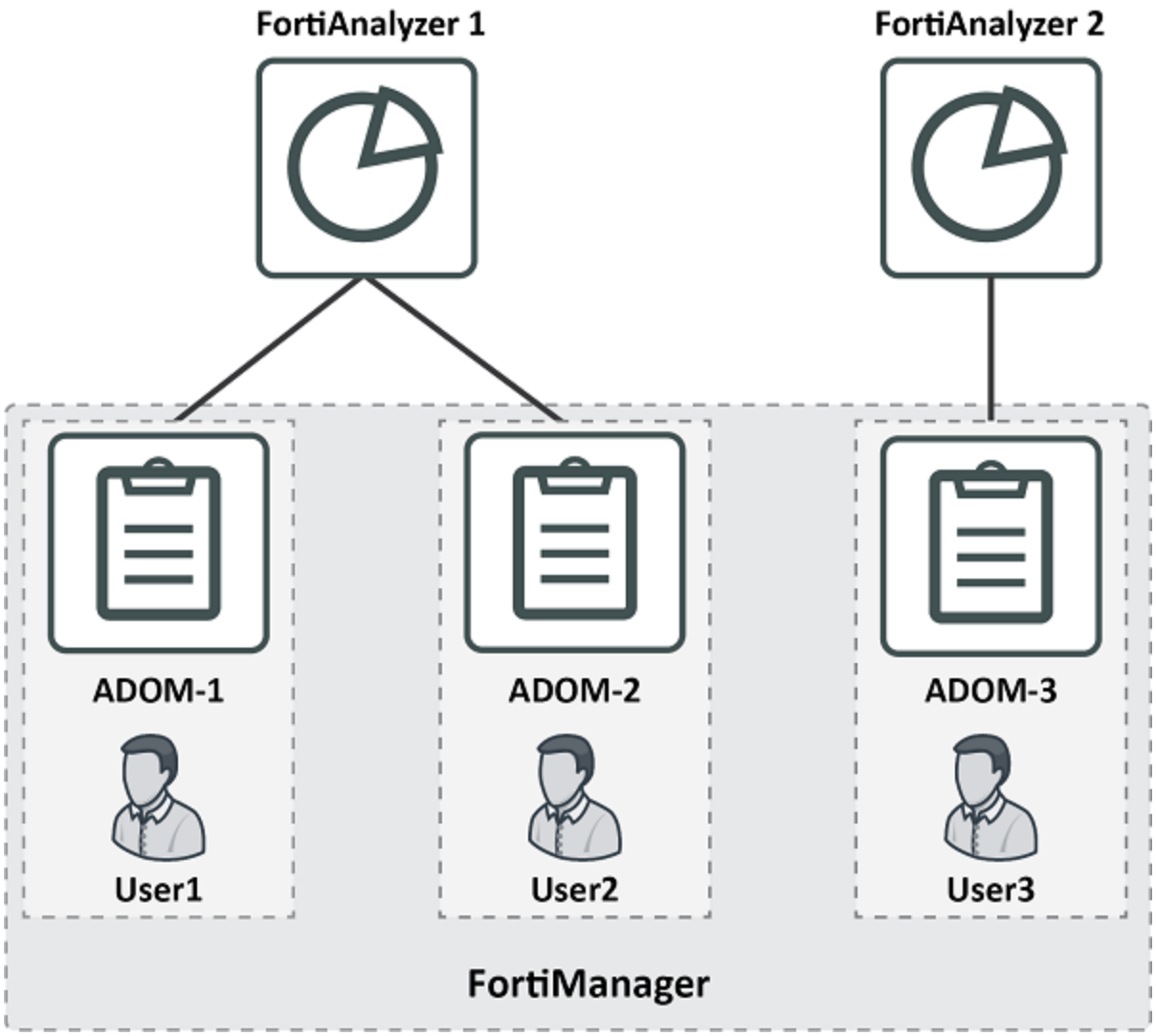
One FortiAnalyzer can be shared across multiple FortiManager ADOMs. While users can see FortiAnalyzer data only from the ADOM they have been assigned to.

### Topology

The scenarios provided below use the following topology which includes three FortiManager ADOMs, and two FortiAnalyzer devices.

- FortiManager ADOM-1 manages FortiAnalyzer device 1.
- FortiManager ADOM-2 manages FortiAnalyzer device 1.
- FortiManager ADOM-3 manages FortiAnalyzer device 2.

Each ADOM has a unique administrator assigned to manage that ADOM. Each administrator can only view their associated ADOM.




## Scenario one: Manage one FortiAnalyzer in multiple ADOMs

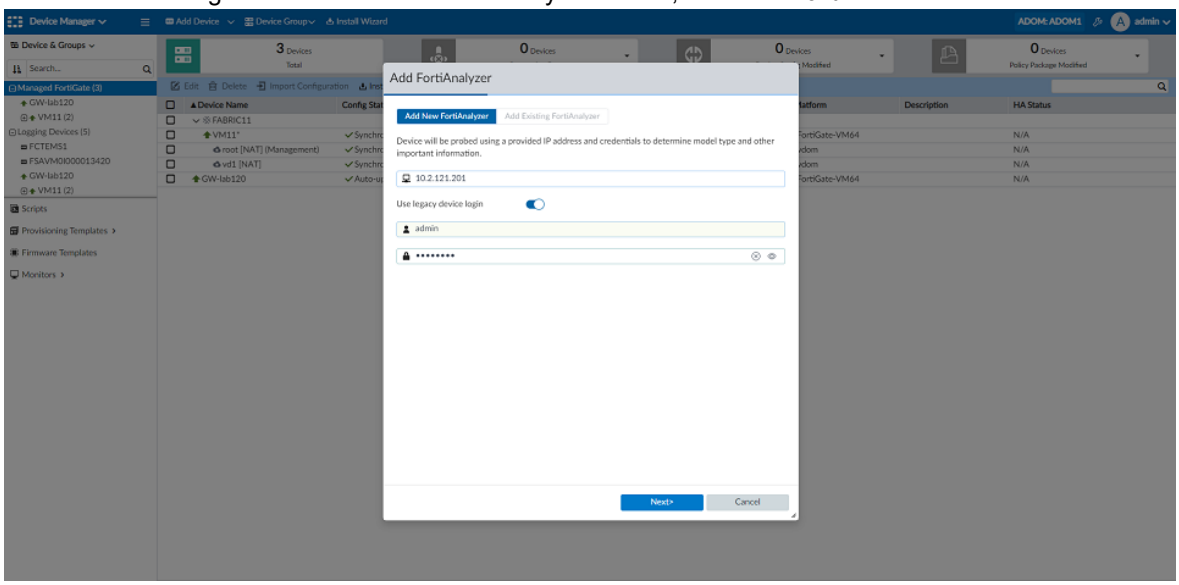
In this example scenario, one FortiAnalyzer device is being managed in two separate FortiManager ADOMs: ADOM-1 and ADOM-2.

Each ADOM has an administrator who is only able to access that ADOM. "User1" can access and manage ADOM-1, and "user2" can access and manage ADOM-2.

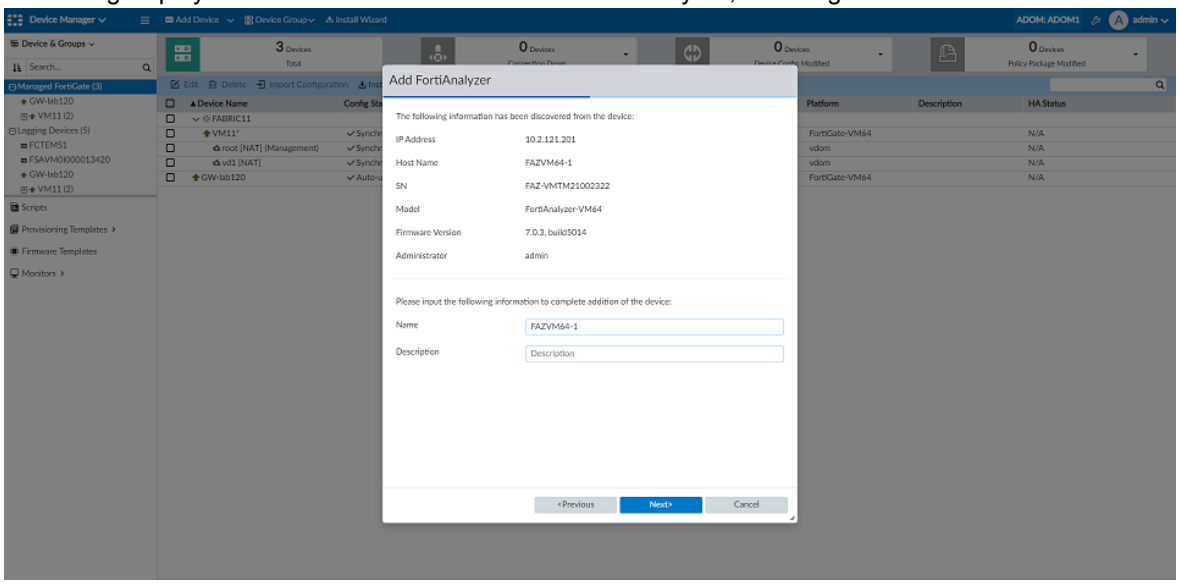
**To configure a managed FortiAnalyzer to serve multiple FortiManager ADOMs:**

1. Add the FortiAnalyzer as a managed device on FortiManager ADOM-1:
   a. In FortiManager, enter ADOM-1.
   b. Go to *Device Manager*, and click *Add Device* > *Add FortiAnalyzer* to add the managed FortiAnalyzer. The *Add FortiAnalyzer* dialog window displays.

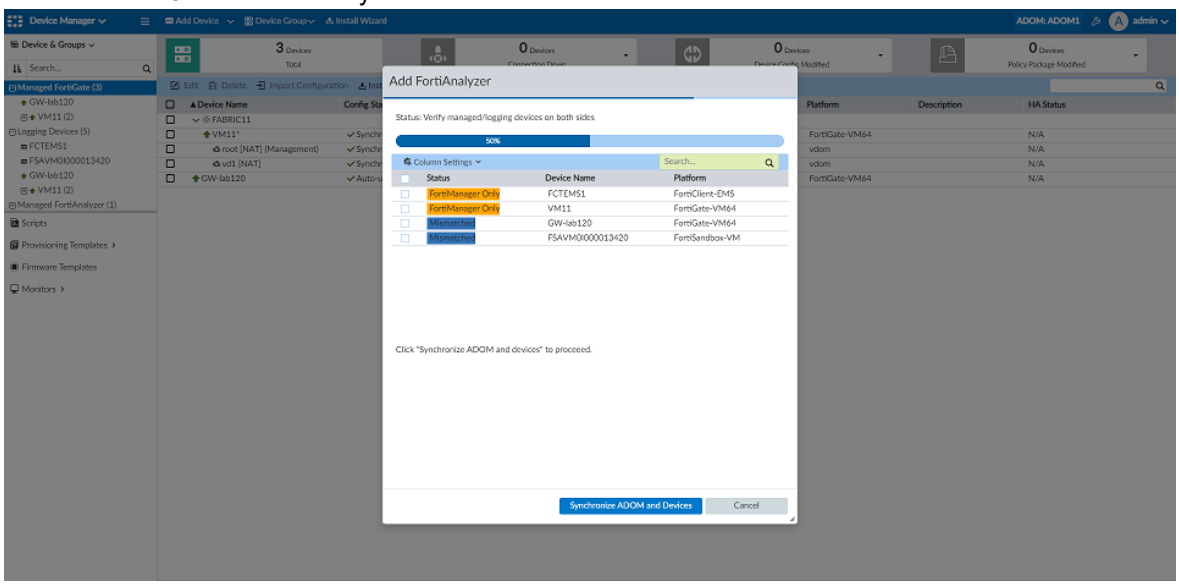
i. Enter the IP and login credentials of the FortiAnalyzer device, and click *Next*.



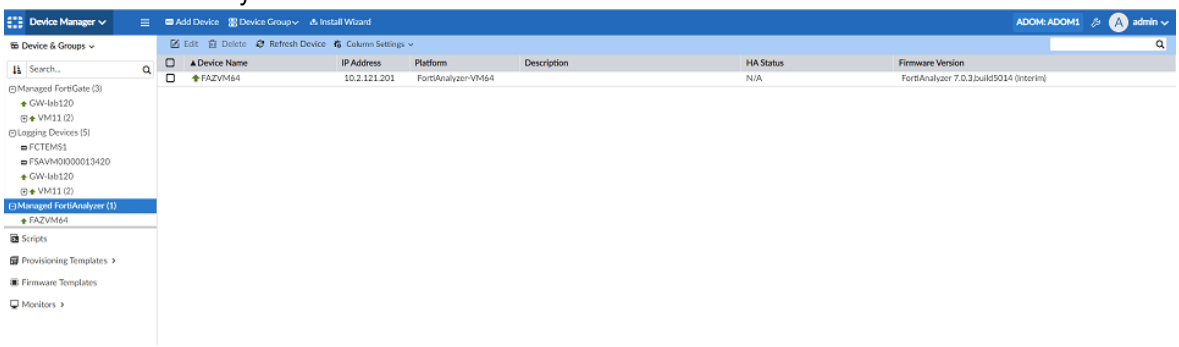

ii. The dialog displays information discovered from the FortiAnalyzer, including the device name. Click *Next*.



iii. Click *Synchronize ADOM and Devices*. After the ADOM and devices are synchronized, the FortiAnalyzer is added to ADOM-1 successfully.

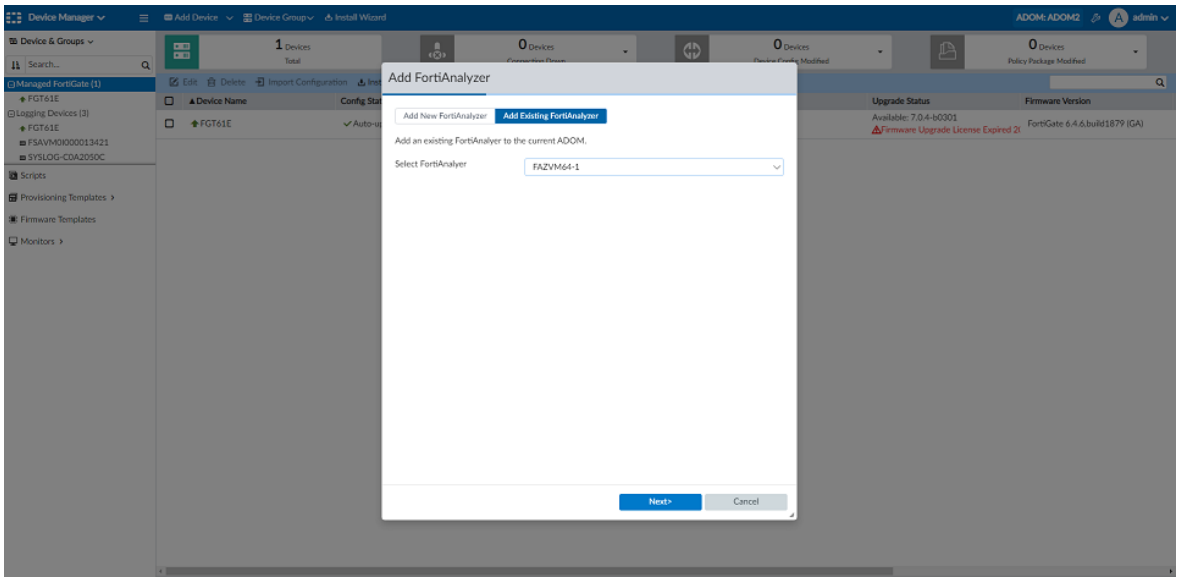



iv. The FortiAnalyzer device can be found under the Managed FortiAnalyzer device group in ADOM-1. You can edit the FortiAnalyzer to view device information.

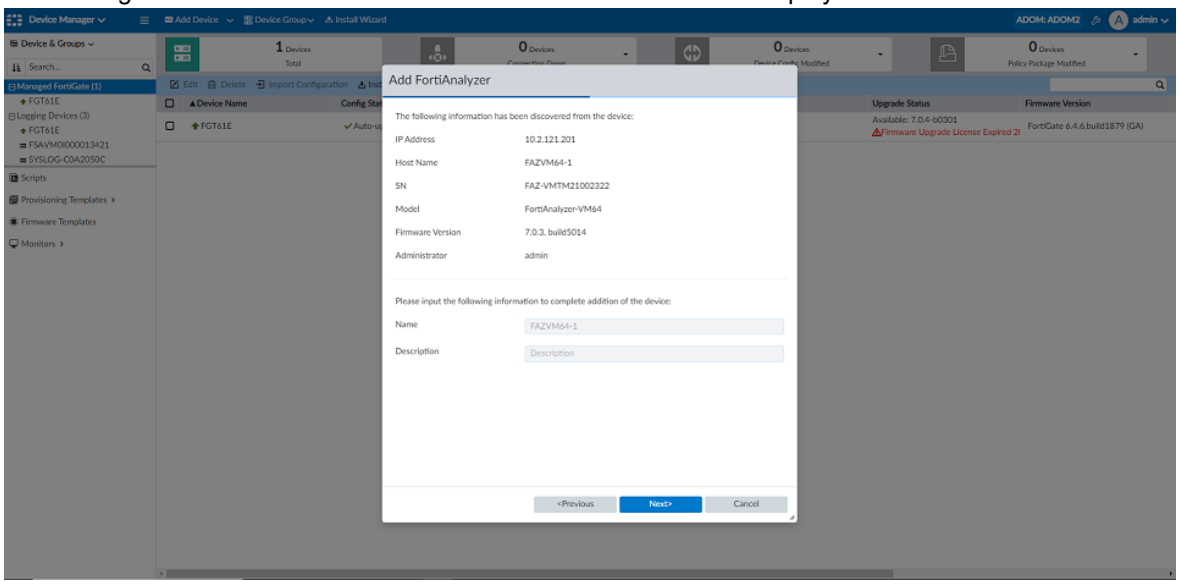


2. Add the FortiAnalyzer as a managed device on FortiManager ADOM-2:
   a. In FortiManager, enter ADOM-2.
   b. Go to *Device Manager*, and click *Add Device* > *Add FortiAnalyzer*. The *Add FortiAnalyzer* dialog window displays.
      i. Click the *Add Existing FortiAnalyzer* tab in the dialog window.

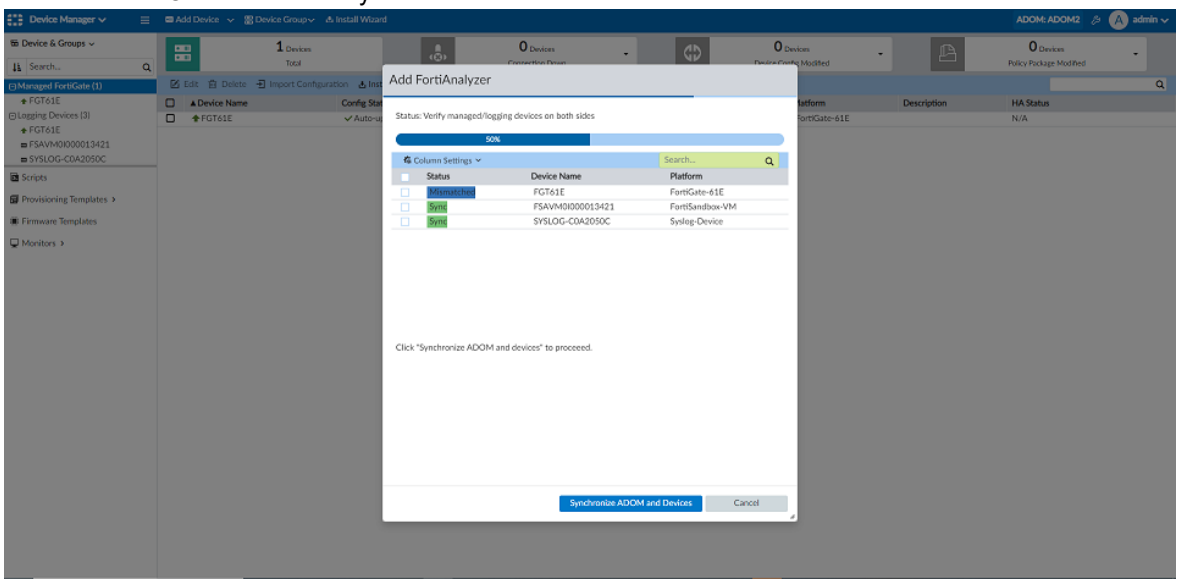
ii. Select the desired FortiAnalyzer from the list of available devices in the *Select FortiAnalyzer* dropdown list, and click *Next*.



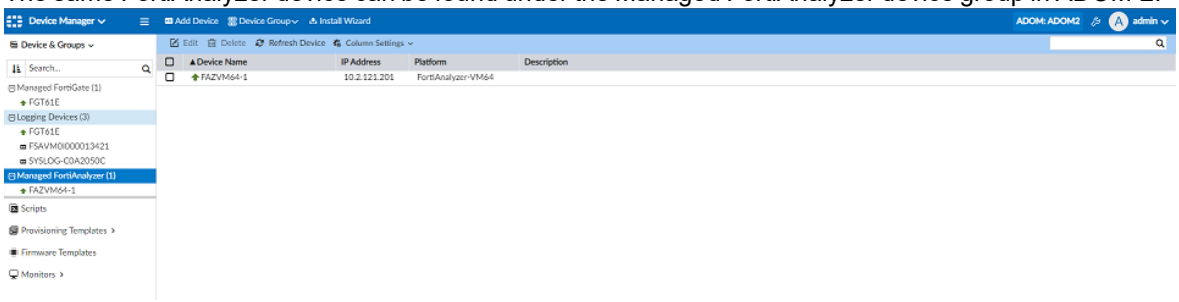

iii. FortiManager will retrieve information from the device database and display it. Click *Next*.



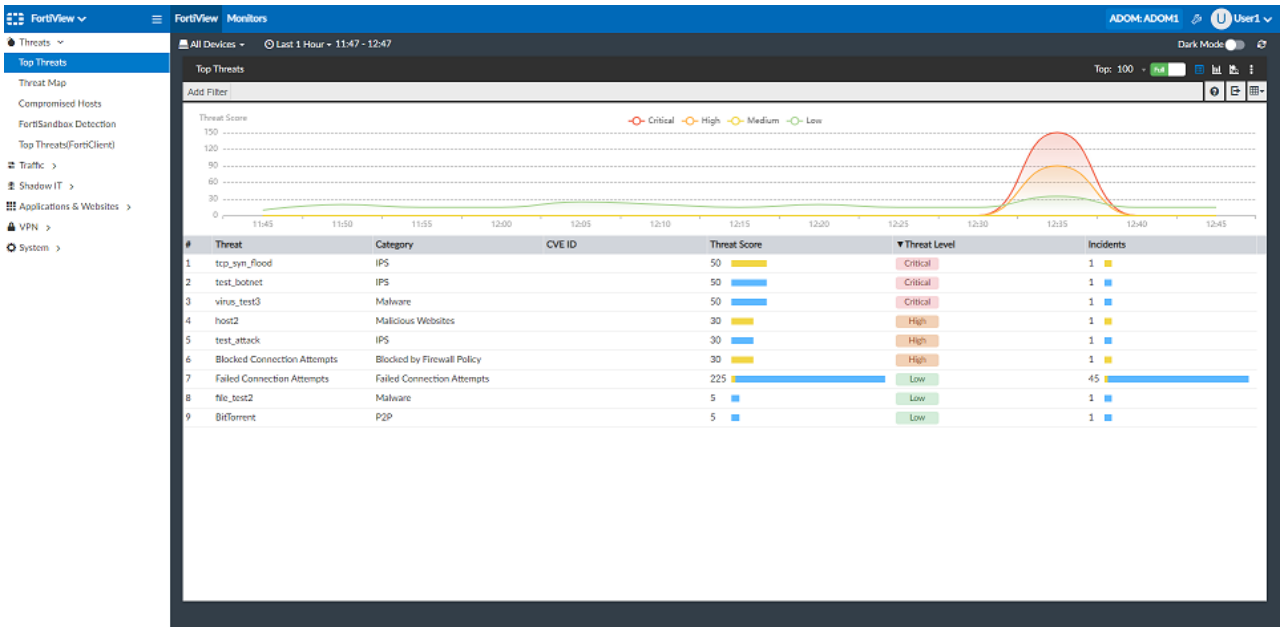
iv. Click *Synchronize ADOM and Devices*. After the ADOM and devices are synchronized, the FortiAnalyzer is added to ADOM-2 successfully.



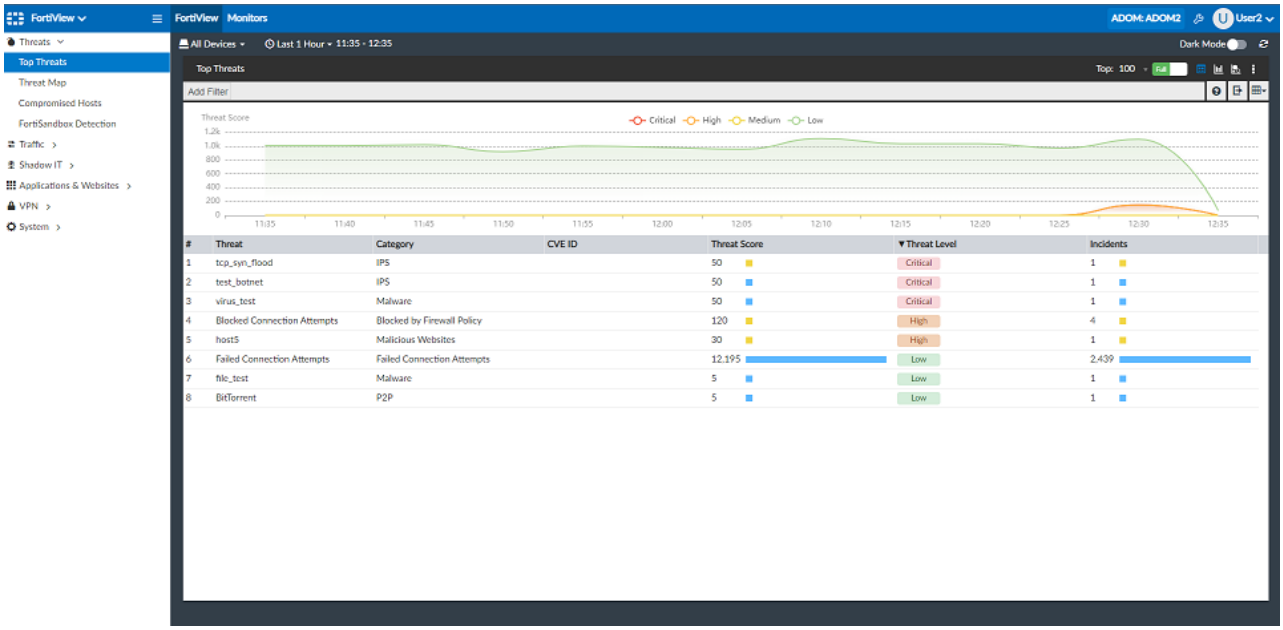

v. The same FortiAnalyzer device can be found under the Managed FortiAnalyzer device group in ADOM-2.




3. Log in to FortiManager with ADOM-1 administrator "User1". In this example scenario, User1 is only allowed to access ADOM-1. When User1 views FortiAnalyzer data, they are only able to see the data related to ADOM-1 devices.



4. Log in to FortiManager with ADOM-2 administrator "User2". In this example scenario, User2 is only allowed to access ADOM-2. When User2 views FortiAnalyzer data, they are only able to see the data related to ADOM-2 devices.




## Scenario two: Manage a second FortiAnalyzer in a new ADOM

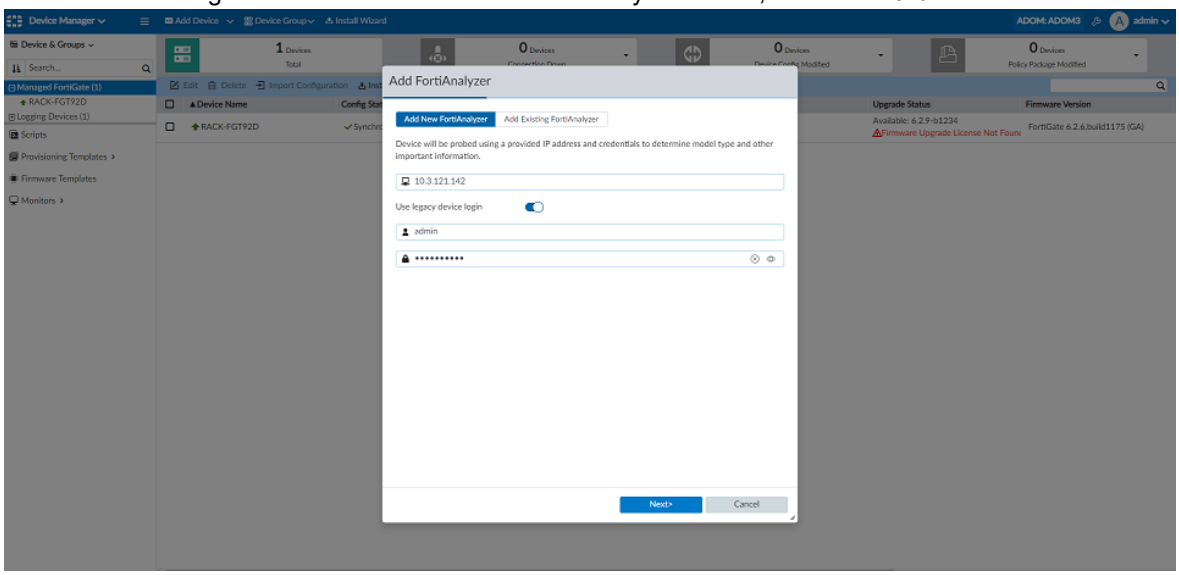
FortiManager can also manage multiple FortiAnalyzer devices in different ADOMs. For example, after one FortiAnalyzer is added to FortiManager ADOM-1 and ADOM-2, a second FortiAnalyzer can be added to ADOM-3.

In this scenario, a second FortiAnalyzer is added to FortiManager ADOM-3, and can be accessed by administrator "user3".

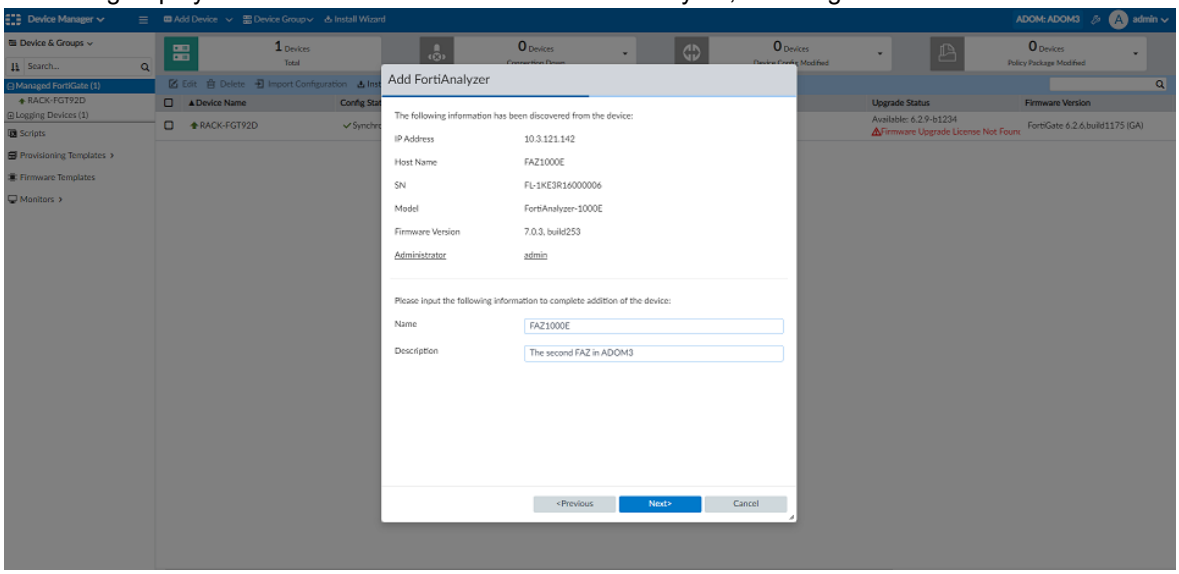
### To manage a second FortiAnalyzer device in FortiManager:

1. Add a second FortiAnalyzer as a managed device on FortiManager ADOM-3:
   a. In FortiManager, enter ADOM-3.
   b. Go to *Device Manager*, and click *Add Device* > *Add FortiAnalyzer* to add the managed FortiAnalyzer. The *Add FortiAnalyzer* dialog window displays.

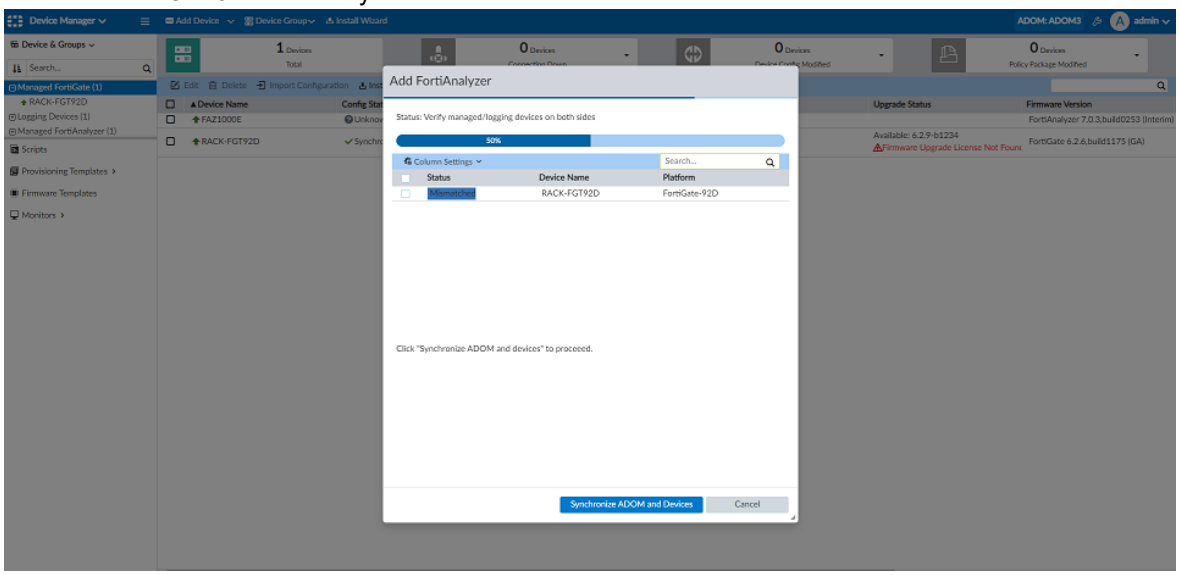
i. Enter the IP and login credentials of the second FortiAnalyzer device, and click *Next*.



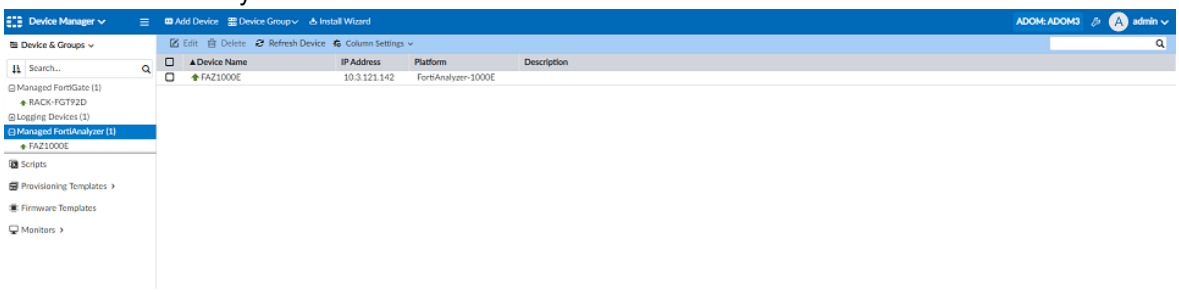

ii. The dialog displays information discovered from the FortiAnalyzer, including the device name. Click *Next*.



iii. Click *Synchronize ADOM and Devices*. After the ADOM and devices are synchronized, the FortiAnalyzer is added to ADOM-3 successfully.

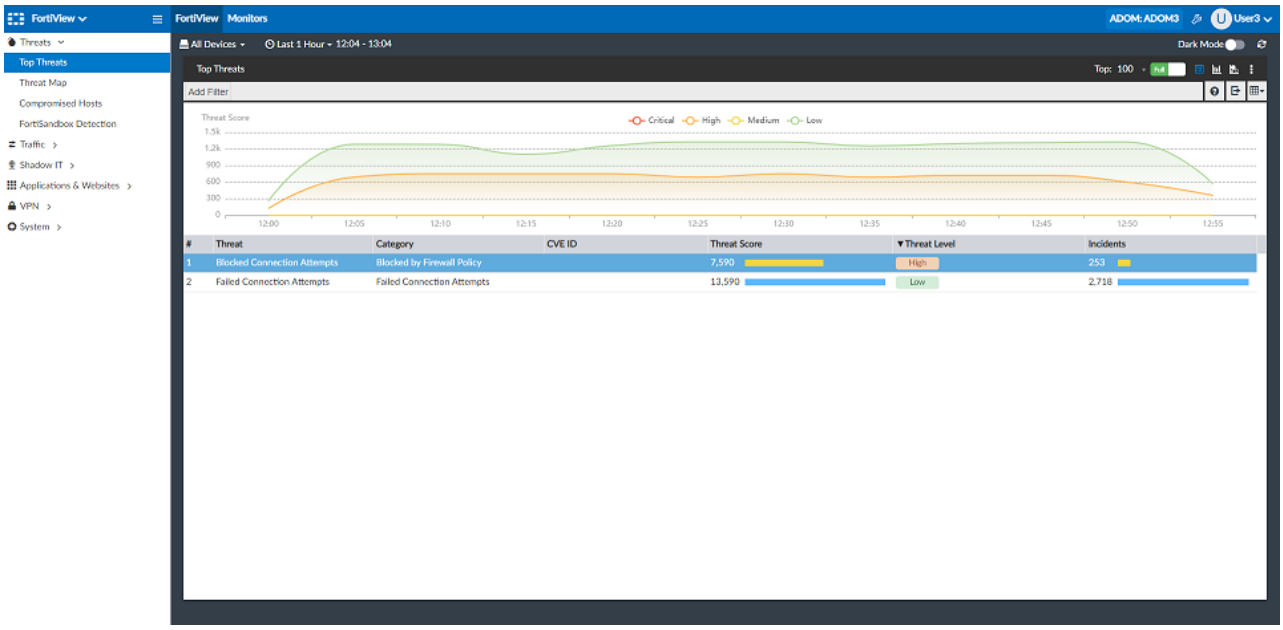



iv. The FortiAnalyzer device can be found under the Managed FortiAnalyzer device group in ADOM-3. You can edit the FortiAnalyzer to view device information.




2. Log in to FortiManager with ADOM-3 administrator "User3". In this example scenario, User3 is only allowed to access ADOM-3. When User3 views FortiAnalyzer data, they are only able to see the data related to ADOM-3

devices.




## SAML SSO wildcard admin user to match all users on IdP server

In FortiManager 7.2.0, you can create a SAML SSO wildcard admin user to match all users on the IdP server.

In the following examples, the IdP is configured with the following local users and profiles:

- *test1* is configured with profile1 which specifies access to adom1.
- *test2* is configured with profile2 which specifies access to adom2.
- *test3* is configured with profile3 which specifies access to all ADOMs.

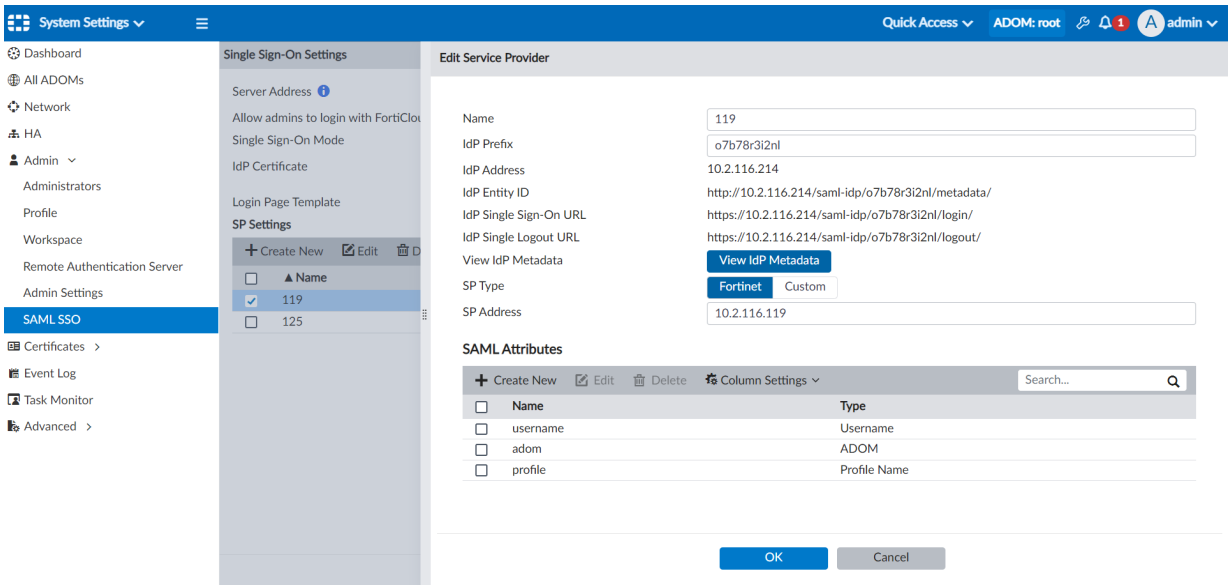
As long as the SP has the same user profile and ADOM names as the IdP, when logging in as an SSO user on the SP, the user is assigned the same profile and ADOMs.

This example assumes that you have already configured SAML SSO in your environment.

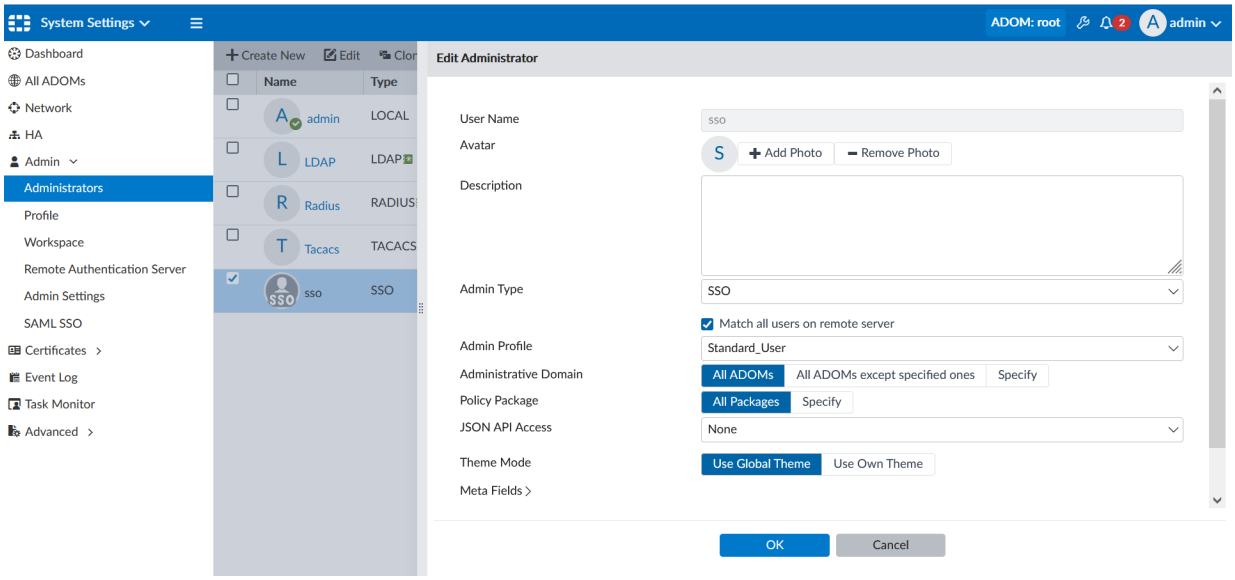
**To configure a SAML wildcard user with SAML attributes:**

1. On the SAML Identity Provider (IdP), click *Create New* under *SP Settings* to configure the service provider.
2. Attributes for the service provider can be added by clicking *Create New* under *SAML Attributes*.
   In this example, the following SAML attributes are used:
   - Name: username, Type: Username
   - Name: adom, Type: ADOM

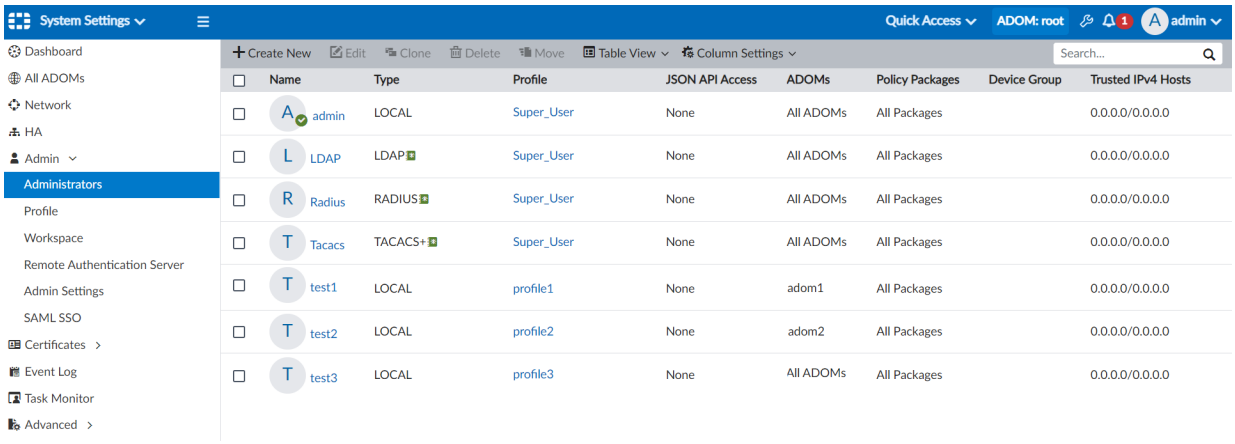
- Name: profile, Type: Profile Name



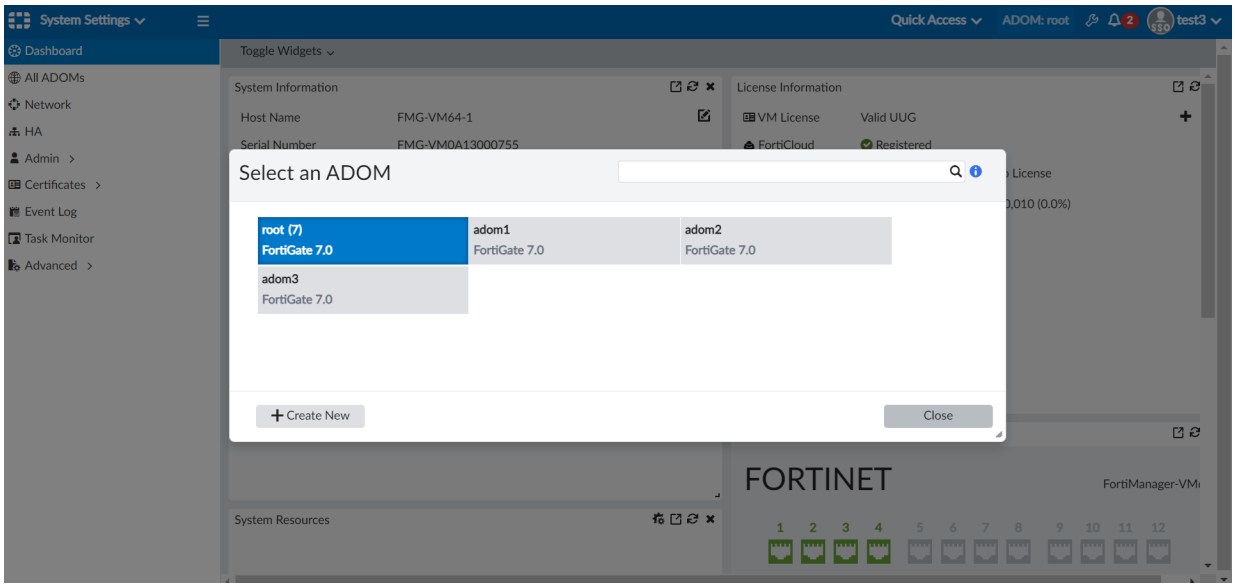

3. On the SAML Service Provider (SP), create one SAML SSO user and enable the *Match all users on remote server* option.




4. Log in to the SP as a local user created on the IdP.
   For example, the local users "test1", "test2", and "test3" have been created on the IdP.




When logging on to the SP as user "test3", the account has the same ADOM access settings as are configured for local user "test3" on the IdP.




## Administrative access to FortiManager controlled by IPv4/IPv6 local-in policy

In FortiManager 7.2.0, administrative access to FortiManager can be controlled by a IPv4/IPv6 local-in policy. This feature can only be configured using the FortiManager CLI.

**To create an IPv4 local-in policy to control administrator access to FortiManager:**

1. Access the FortiManager CLI.
2. Enter the following command to create the IPv4 local-in policy:

```
config system local-in-policy
   (local-in-policy)# edit <policy ID>
   new entry '<Policy ID>' added
```

3. Configure additional settings for the local-in policy using the `set` command. For example:

```
set
   action Action performed on traffic matching this policy.
```

```
    dport Destination port number (0 for all).
    dst Destination IP and mask.
    intf Incoming interface name.
    protocal Traffic protocal.
    src Source IP and mask.
```

**To create an IPv6 local-in policy to control administrator access to FortiManager:**

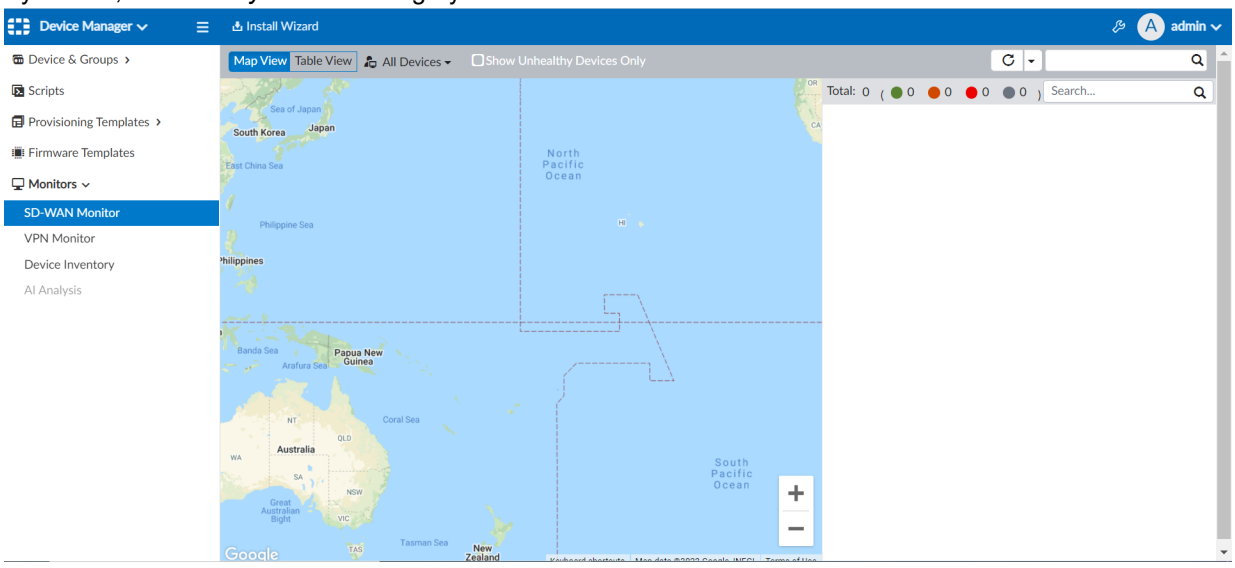
1. Access the FortiManager CLI.
2. Enter the following command to create the IPv6 local-in policy:
   ```
   config system local-in-policy6
      (local-in-policy6)# edit <policy ID>
      new entry '<Policy ID>' added
   ```
3. Configure additional settings for the local-in policy using the `set` command.
   For example:
   ```
   set
      action Action performed on traffic matching this policy.
      dport Destination port number (0 for all).
      dst Destination IP and mask.
      intf Incoming interface name.
      protocal Traffic protocal.
      src Source IP and mask.
   ```

## AI Analysis link exposed in Device Manager redirects to FortiAIOps MEA

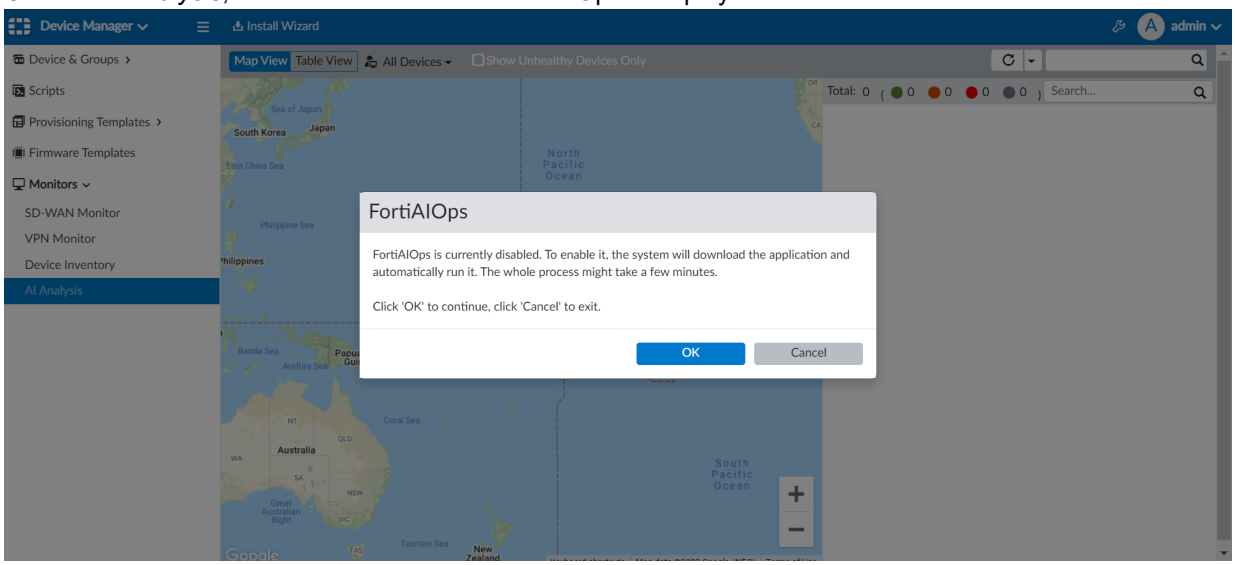
A new AI Analysis link added in Device Manager redirects to FortiAIOps management extension.

**To view FortiAIOps analysis from FortiManager:**

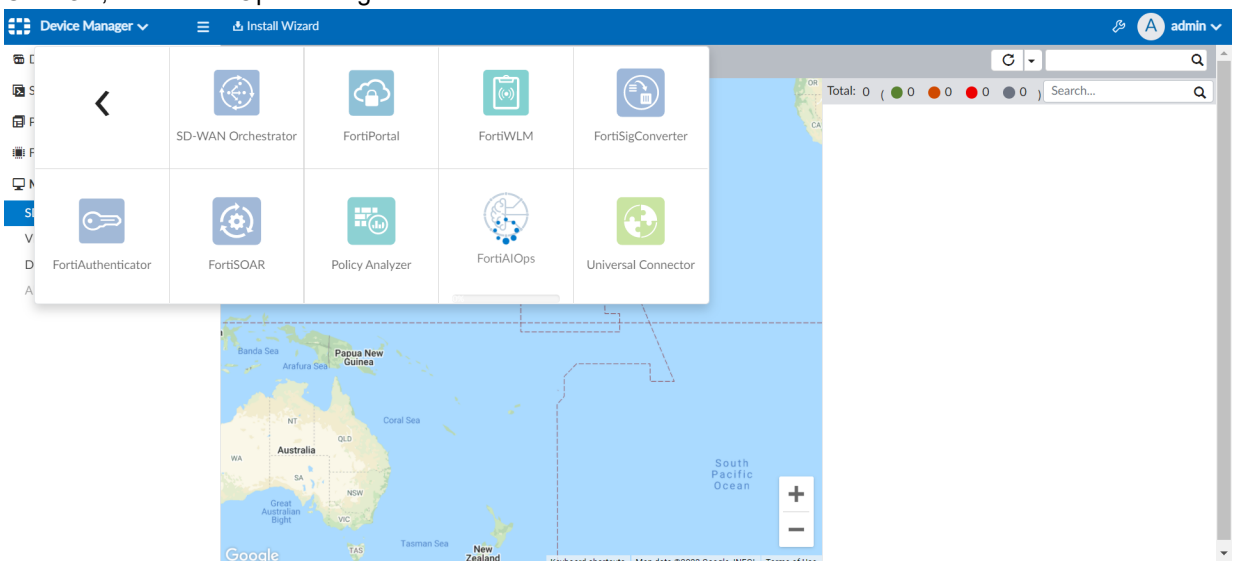
1. In FortiManager, go to *Device Manager* > *Monitors*.
   By default, the *AI Analysis* monitor is grayed out.



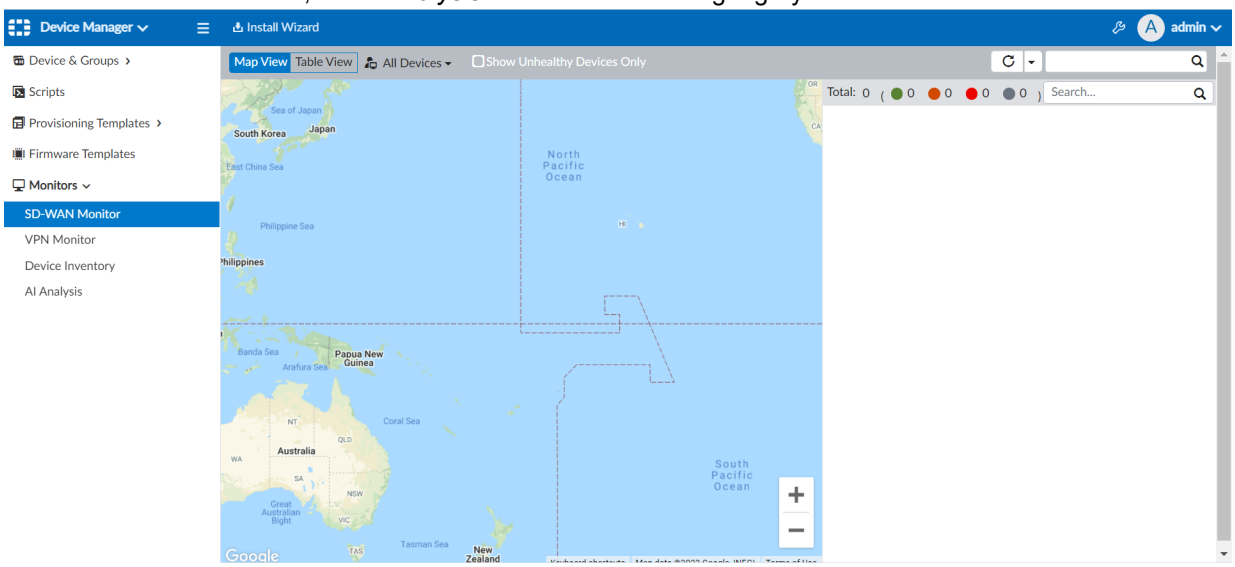
2. Click on *AI Analysis*, and a window to enable FortiAIOps is displayed.



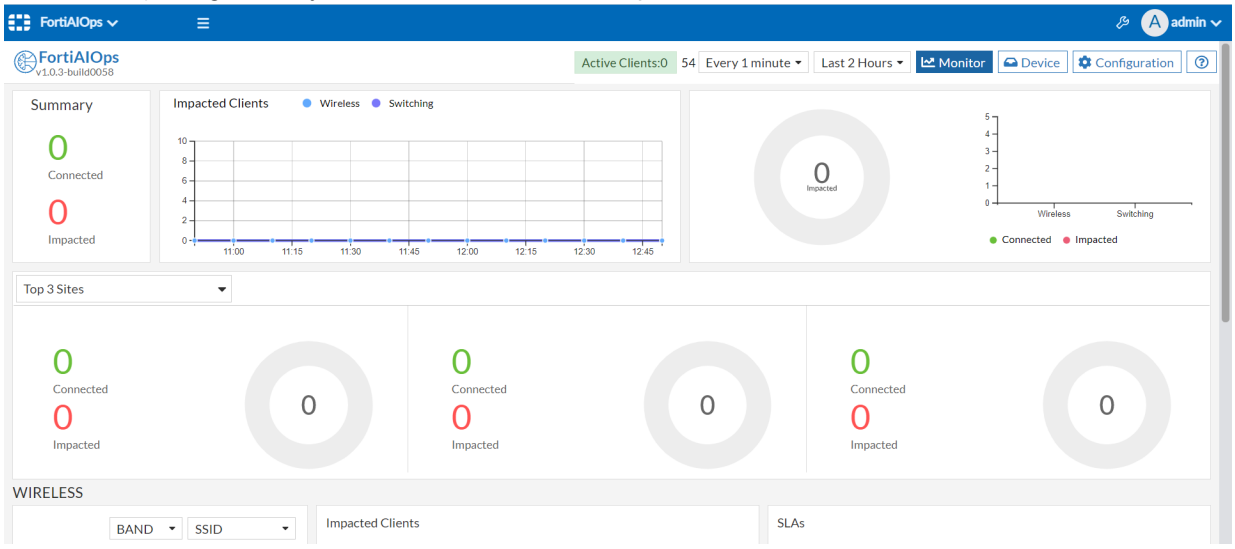

3. Click *OK*, and ForitAIOps will begin to download.



4. After the download finishes, the *AI Analysis* monitor link is no longer grayed out.




5. Click *AI Analysis* again and you are redirected to FortiAIOps.

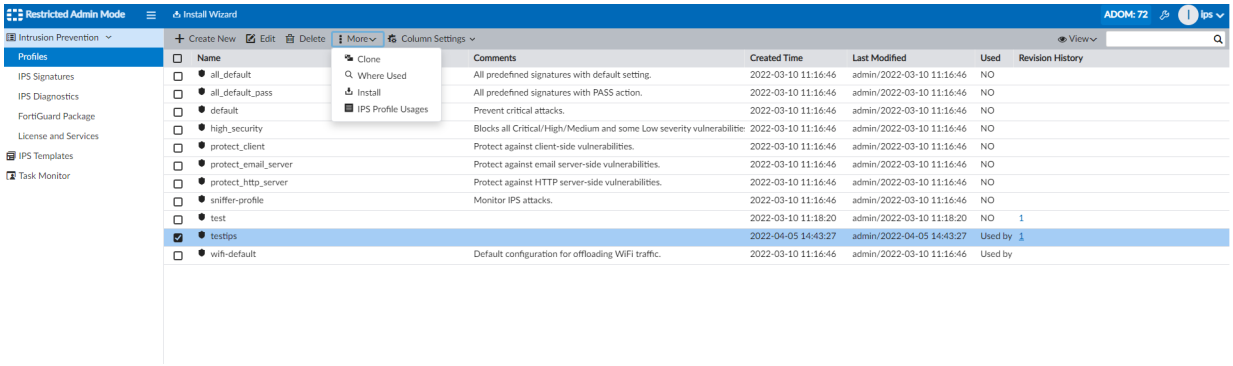



## IPS administrators have visibility on each IPS profile

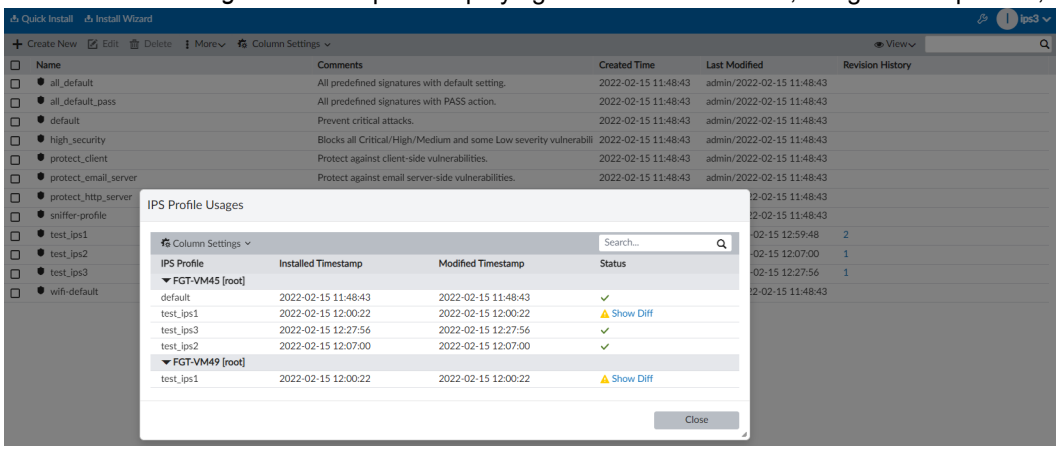
IPS administrators have visibility on each IPS profile including usage, status, installed vs. modify, and side-by-side configuration diffs.

**View IPS sensor status changes as an IPS administrator:**

1. Log in to FortiManager as a restricted IPS administrator.
2. Go to *Intrusion Prevention* > *Profiles*.




3. In the toolbar, click *More* > *IPS Profile Usages*.
   The *IPS Profile Usages* window opens displaying the FortiGate devices, assigned IPS profiles, and sync status.

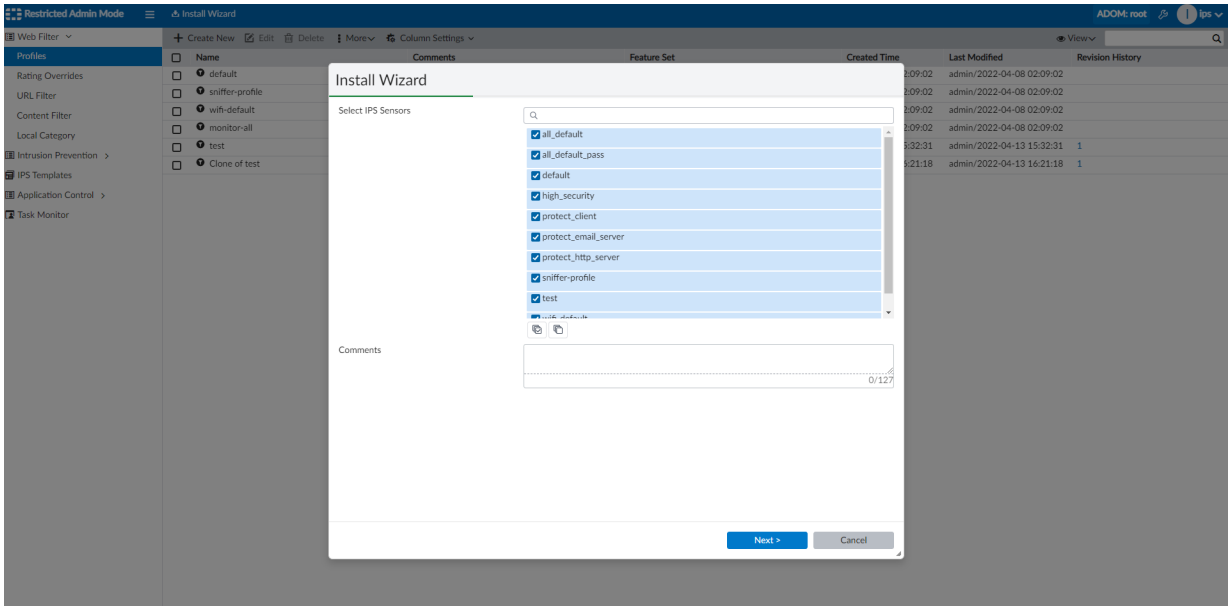



## IPS admin install preview for multiple FortiGate devices at once shows the CLI configuration to be installed on each target device

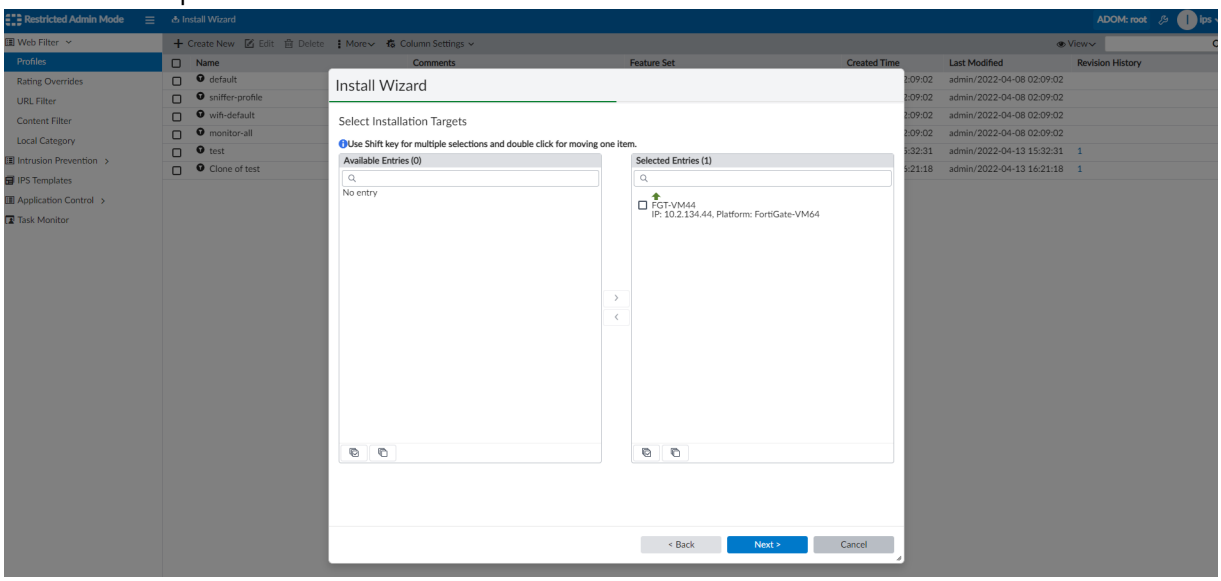
IPS admin install preview for multiple FortiGate devices at once displays the CLI configuration to be installed on each target device.

**To view the CLI configuration to be installed on target devices:**

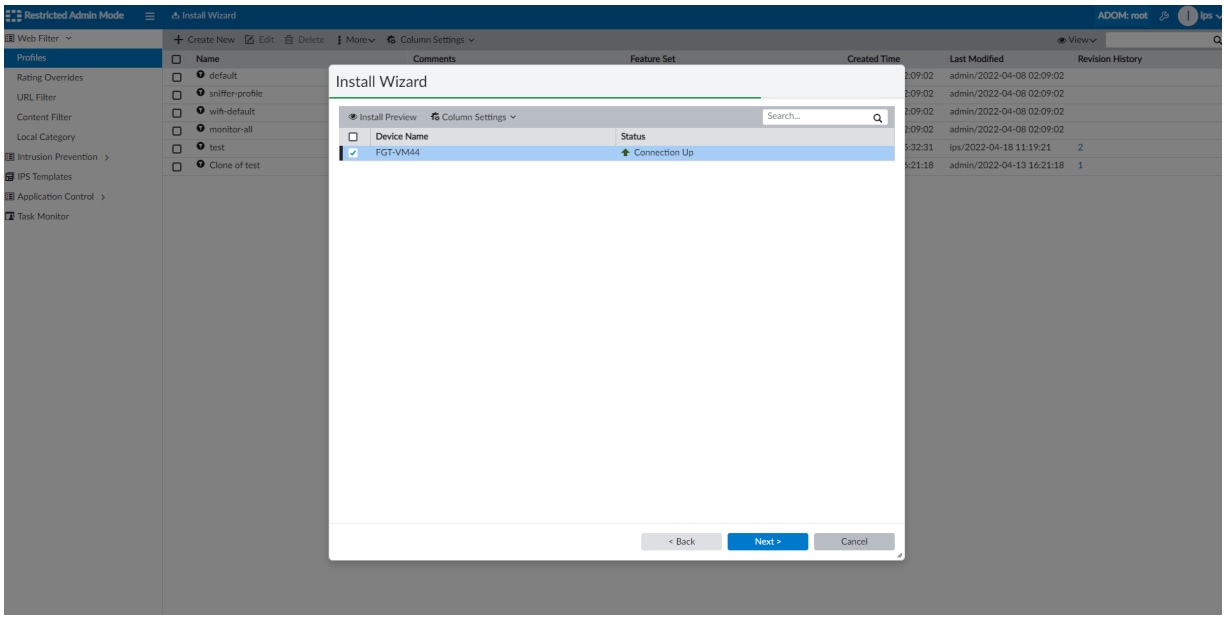
1. Log in as a restricted IPS administrator.
2. Go to the *Install Wizard*.



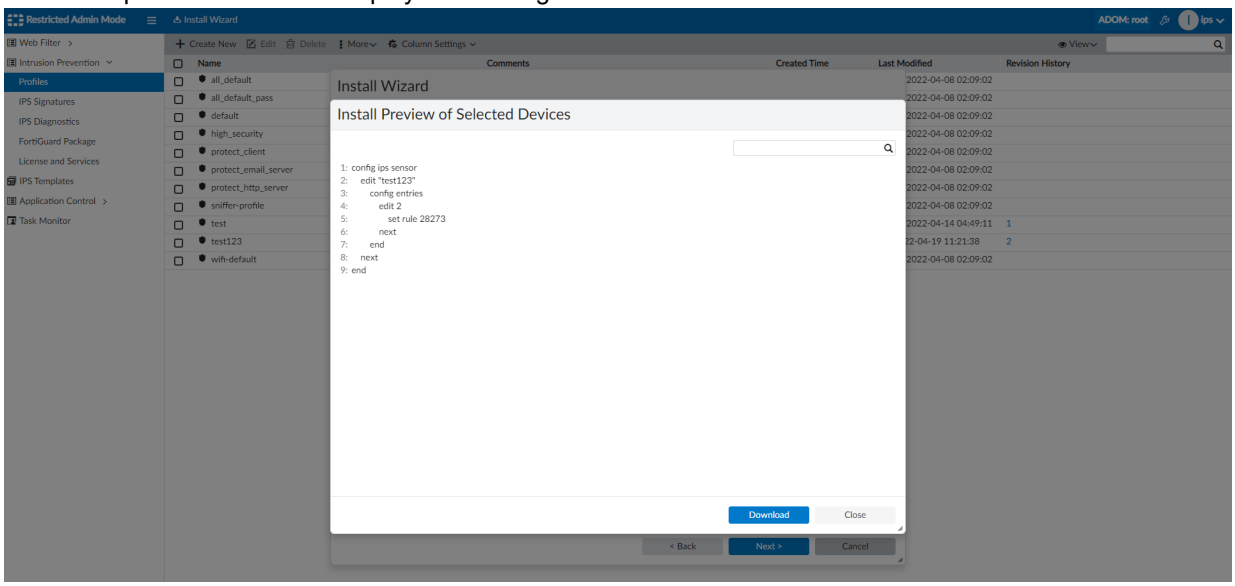

3. Add a device to perform the installation on.



4. Select a device from the list, and click *Install Preview*.




The install preview details are displayed including the CLI to be installed on the selected device.

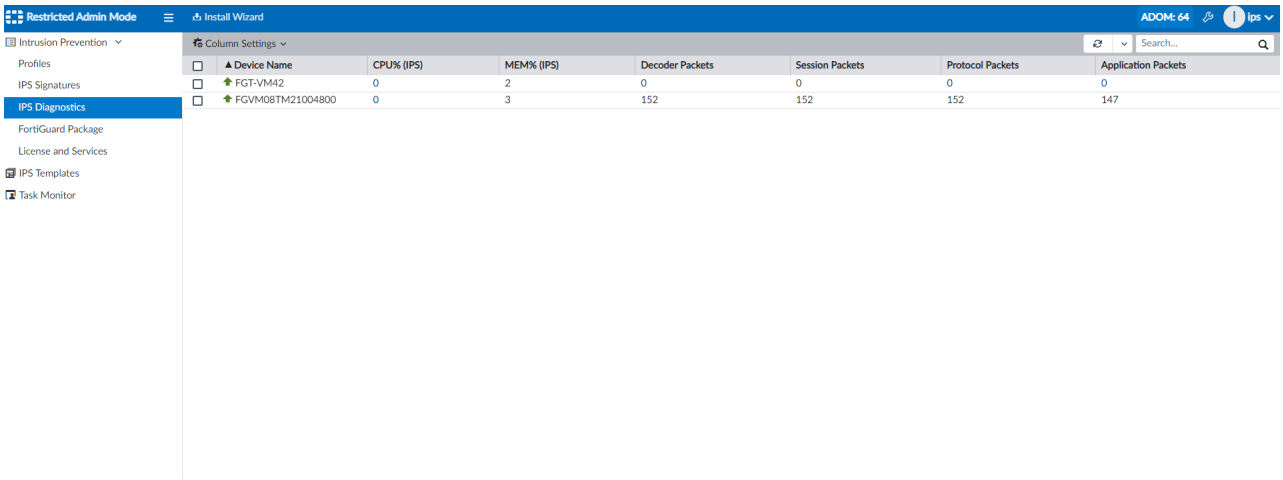



## IPS diagnostics page for IPS dedicated admin displays CPU, memory, and performance statistics for FortiGates related to IPS processes

IPS diagnostics page for IPS dedicated admin displays CPU, Memory, and performance statistics for FortiGates related to IPS processes.

**To view IPS Diagnostics as an IPS administrator:**

1. Log in to FortiManager as an IPS administrator.
2. Go to *Intrusion Prevention* > *IPS Diagnostics*.
   The *IPS Diagnostics* page is displayed.




FortiManager uses FortiOS APIs to get information, then calculates the CPU, memory, and performance statistics for IPS processes.

## IoT query service support - 7.2.1

When FortiManager acts as a management update server to managed FortiGates for the Internet of Things (IoT) Device Identification service, FortiManager sends the IoT collection reports from FortiGate to FortiGuard Distribution Server (FDS).

When FortiManager acts as an FDS in closed networks, you can use the following network design modes: cascade mode or air gap mode. For FortiManager devices in cascade mode that are managing FortiGates with the IoT Device Identification service, you must set `service-type` to `iot-collect` on the downstream FortiManager devices to enable them to send the IoT collection reports from FortiGates to the upstream FortiManager device to send to FDS.

For more information about the network design modes in closed networks, see the *FortiManager Best Practices Guide*. For information about using the built-in FDS available with FortiManager, see the *FortiManager 7.2 Administration Guide*.

**To enable sending of IoT collection reports to FDS:**

1. Enable IoT services for query and collect:

```
config fmupdate service
    set query-iot enable
end
```

2. If you are using FortiManager devices in cascade mode in a closed network, set the `service-type` to `iot-collect` on downstream FortiManager devices:

```
config fmupdate web-spam fgd-setting
    config server-override
        set status enable
            config servlist
                edit 1
                        ......
                        set service-type iot-collect
                    next
                end
```

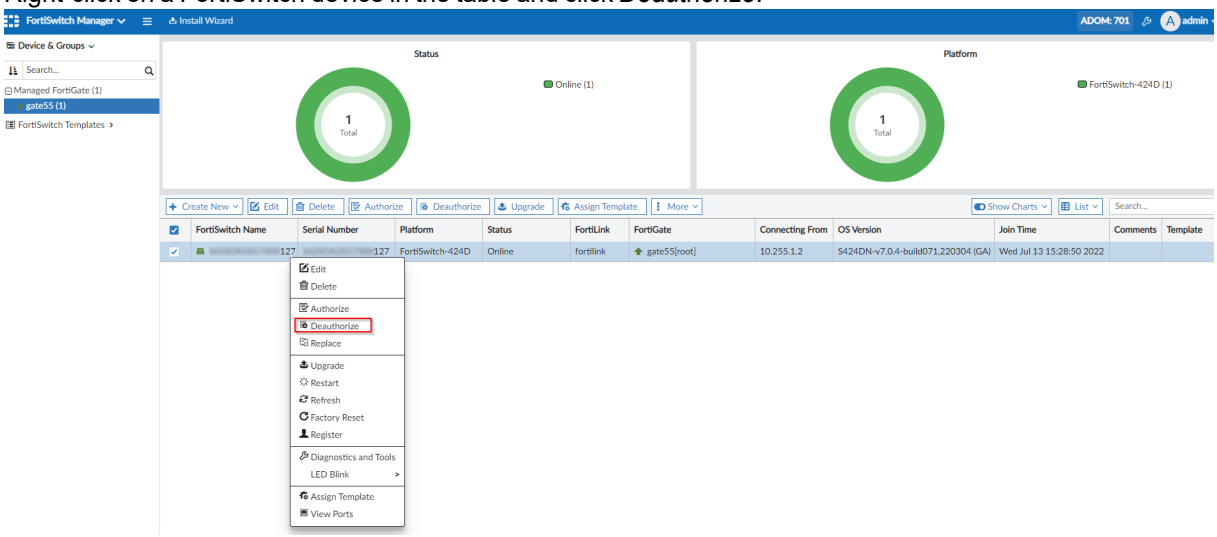
```
        end
end
```

## Initiate the RMA process to replace the FortiSwitch or FortiAP units from FortiManager - 7.2.1

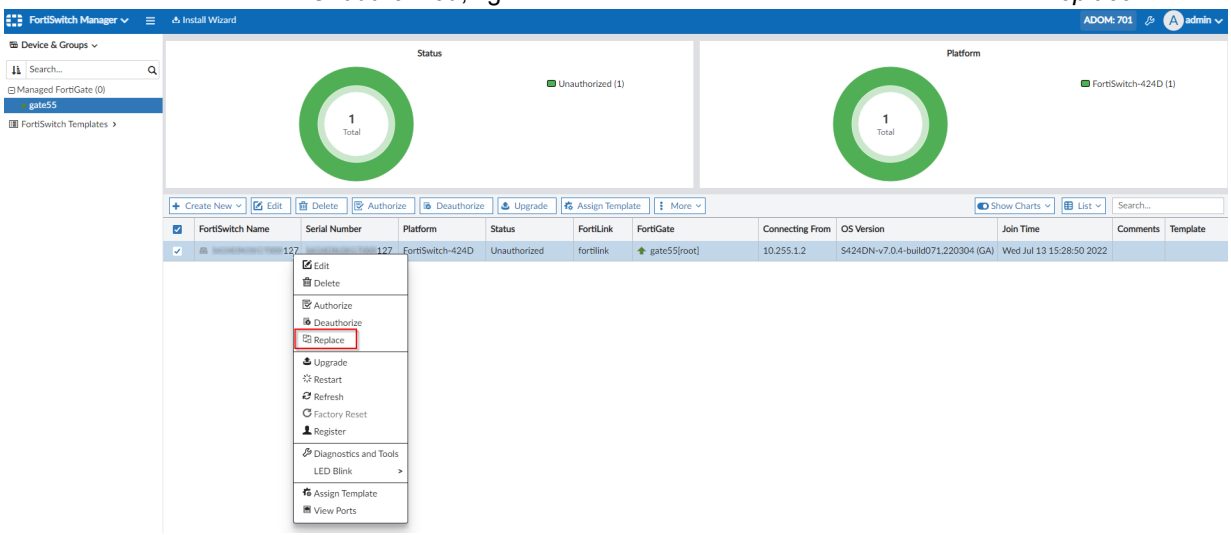
In FortiManager 7.2.1, you can initiate the RMA process to replace the FortiSwitch or FortiAP units from FortiManager.

**To replace a FortiSwitch device in FortiManager:**

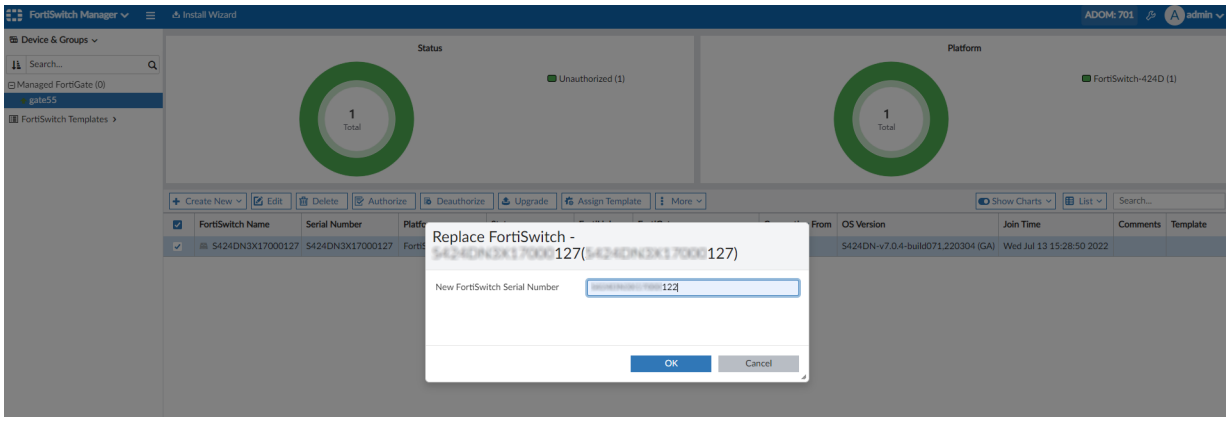
1. Go to *FortiSwitch Manager* > *Device & Groups*, and select a managed FortiGate.
2. Right-click on a FortiSwitch device in the table and click *Deauthorize*.



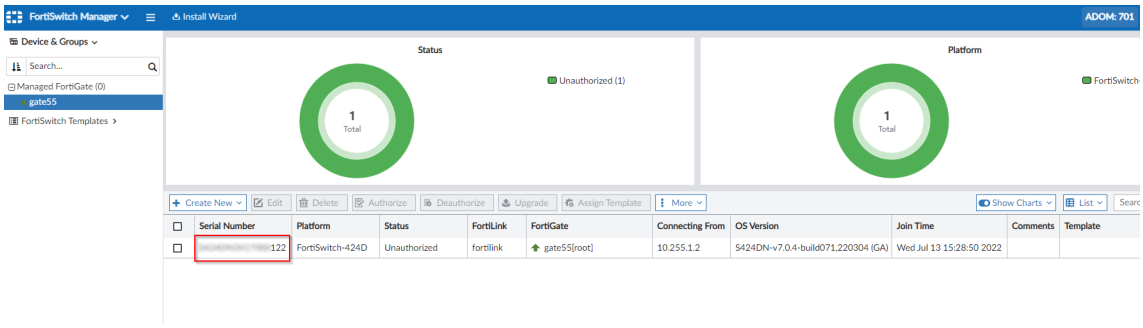

3. When the device's status is *Unauthorized*, right-click on the same FortiSwitch device and click *Replace*.



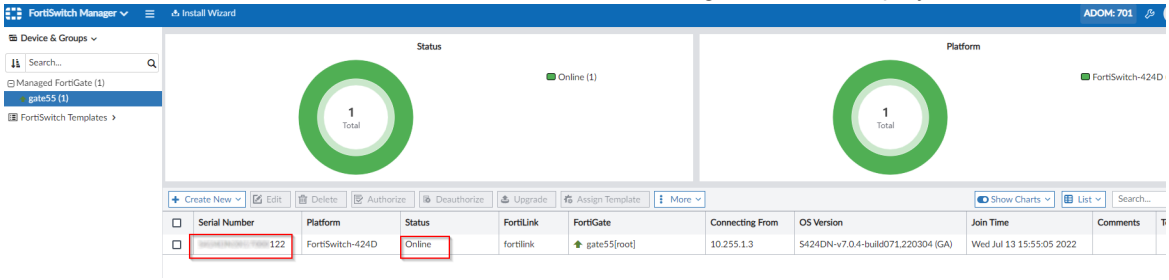
4. Enter the new FortiSwitch serial number, and click *OK*.




After the FortiSwitch has been replaced successfully, refresh the page and the new FortiSwitch is displayed as *Unauthorized*.

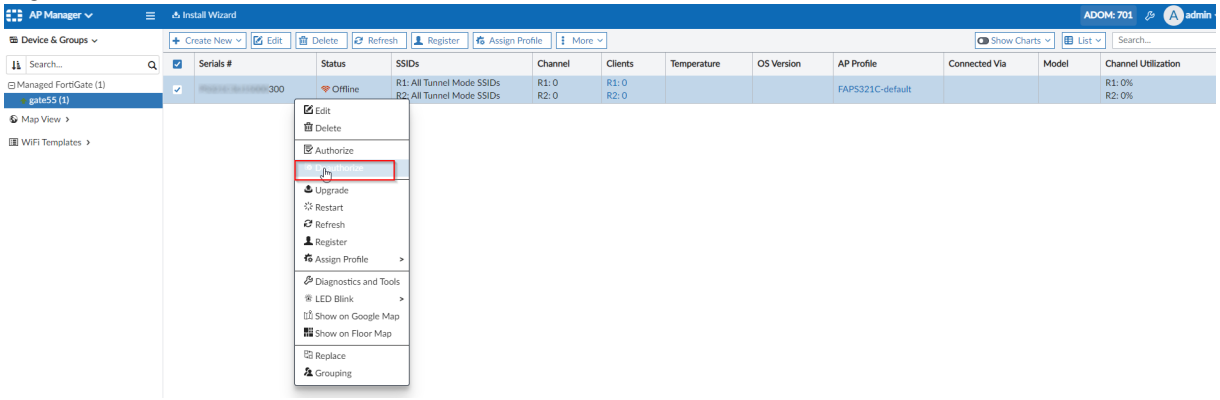



5. Authorize the FortiSwitch device, then connect the FortiSwitch to the FortiGate.
6. Power on the FortiSwitch device. After a few minutes, the managed switch is displayed as *Online*.

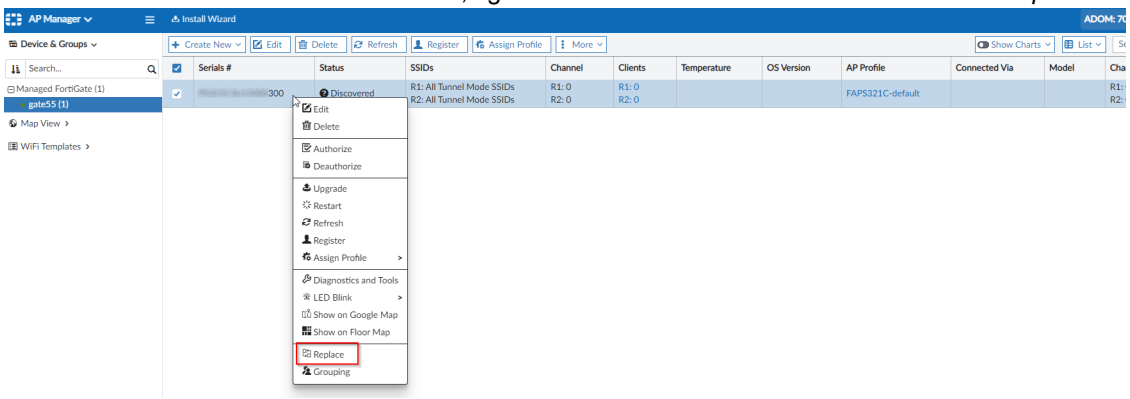


### To replace a FortiAP device in FortiManager:

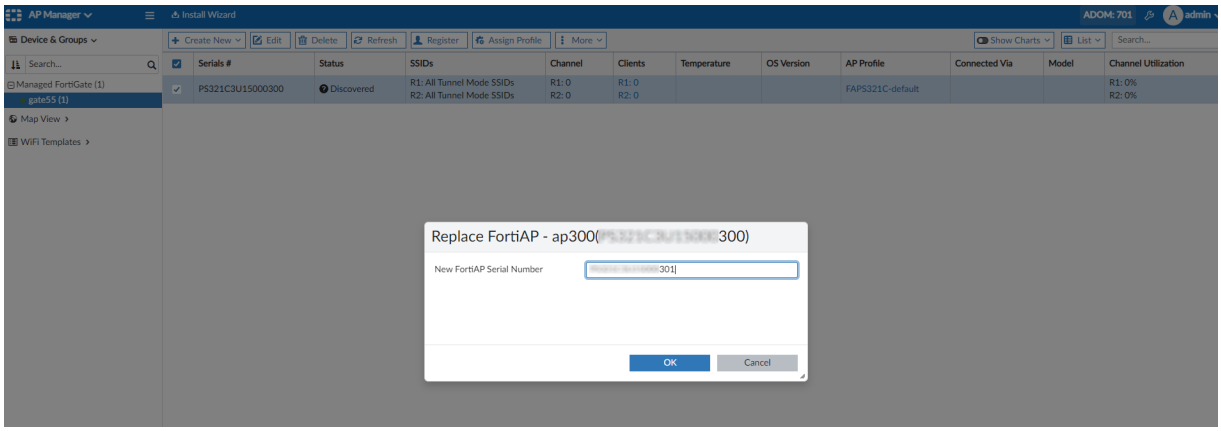
1. Go to *AP Manager* > *Device & Groups*, and select a managed FortiGate.
2. Right-click on a FortiAP device in the table and click *Deauthorize*.



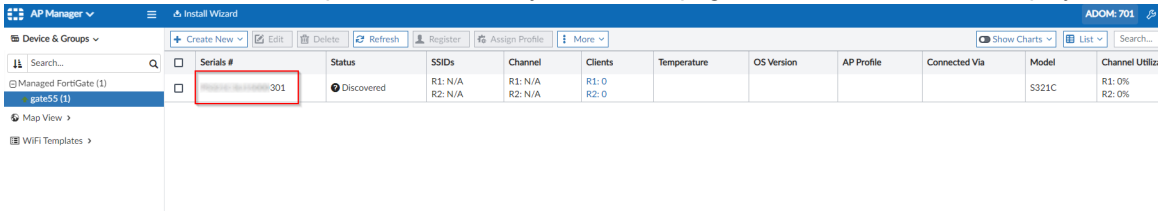

3. When the device's status is *Unauthorized*, right-click on the same FortiAP device and click *Replace*.



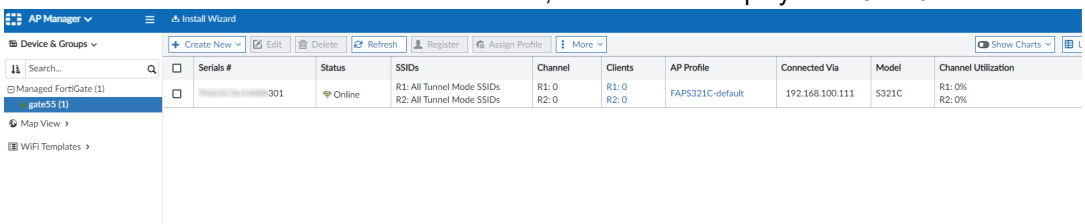

4. Enter the new FortiAP serial number, and click *OK*.




After the FortiAP has been replaced successfully, refresh the page and the new FortiAP is displayed.



5. Authorize the FortiAP device, then connect the FortiAP to the FortiGate.
6. Power on the FortiAP device. After a few minutes, the FortiAP is displayed as *Online*.

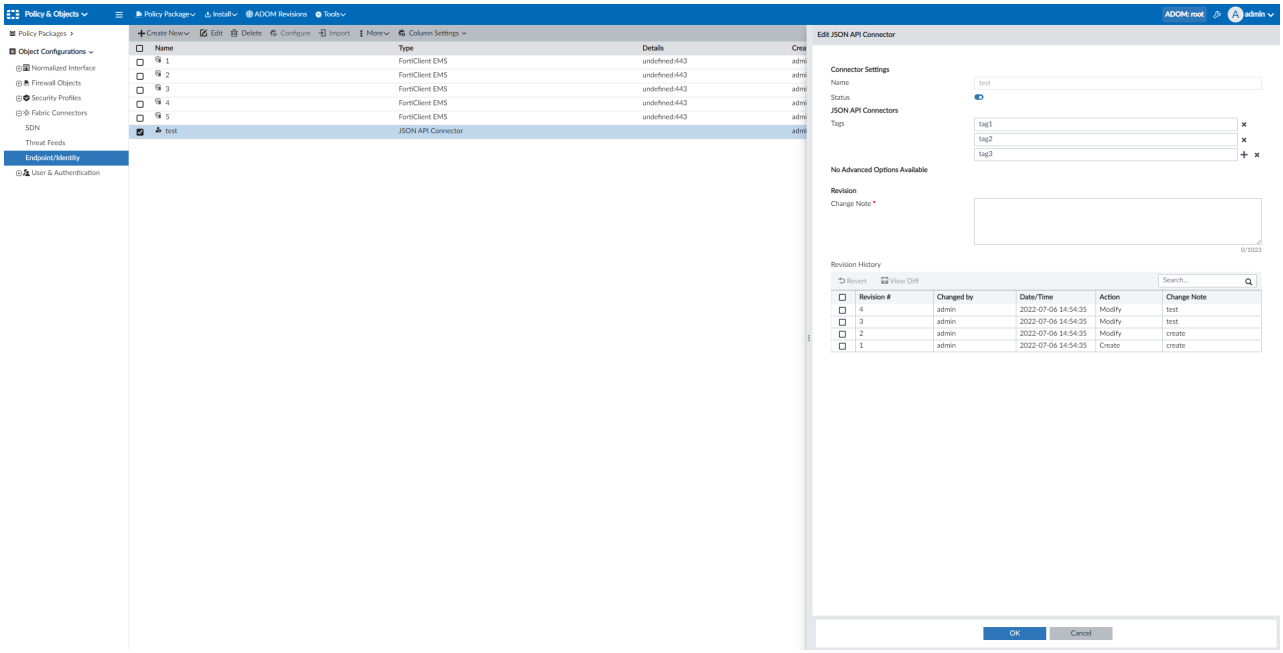



## FortiManager supports push updates via JSON API for dynamic address groups objects - 7.2.1

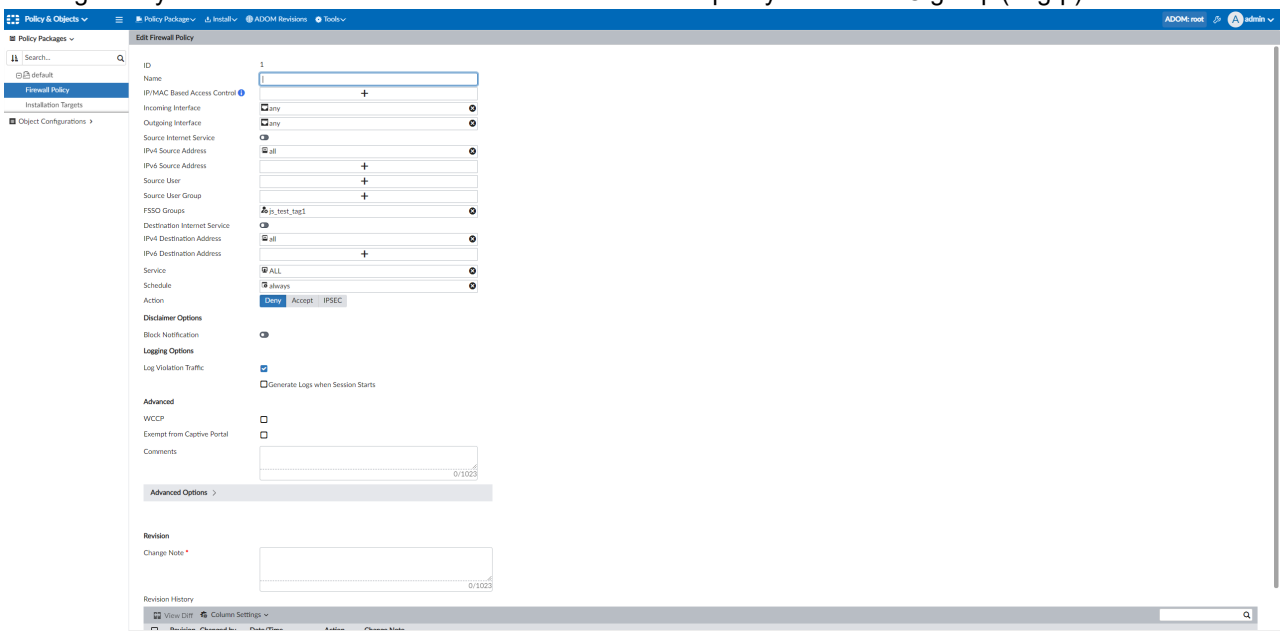
FortiManager supports push updates via JSON API for dynamic address groups objects which are not reachable directly to address customers isolated VM infrastructure and role separation cases.

**To create a JSON API connector:**

1. Go to *Fabric View* and click *Create New* > *JSON API connector*.
   You can also configure this connector at *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *Endpoint/Identity*.
   Configure the connector details, and add the tags.
2. Click *OK* to save the connector.



3. The tags that you created in the connector can now be used in a policy as the FSSO group (adgrp).




4. Install the policy with the FSSO group to FortiGate.
Once the policy with the FSSO group(s) are installed on a FortiGate, you can use the JSON API to operate the connector to add users, get FSSO groups, get users, or delete users.
For example:

- **To manage users:**


```
{
                                                    "method": "exec",
                                                    "params": [
                                                    {
                                                    "data": {
                                                    "command": "add",
                                                    "path": "root/test",
                                                    "group": "tag1",
                                                    "ip-addr": [
                                                    "1.1.1.1",
                                                    "2.2.2.2"
                                                    ]
                                                    },
                                                    "url": "/connector/user/manage"
                                                    }
                                                    ],
                                                    "session":
"3wiI3MoD4JA6Rfj+ue0sqwqcxg8ND/+XM3iAviX7FJtpVJi6e+bATeipvbePTDgK2h/xbJGyY0g=="
                                                    }

                                                    {
                                                    "result": [
                                                    {
                                                    "status": {
                                                    "code": 0,
                                                    "message": "OK"
                                                    },
                                                    "url": "/connector/user/manage"
```

```
                                                                }
                                                                ]
                                                        }
```

- **To get FSSO groups (adgrp):**

```
{
                                                                "method":"exec",
                                                                "params":[
                                                                {
                                                                "data":{
                                                                "adom":"root",
                                                                "connector":"test",
                                                                "server_type":"json"
                                                                },
                                                                "url":"\/connector\/get\/adgrp"
                                                                }
                                                                ],
                                                                "session":
"3wiI3MoD4JA6Rfj+ue0sqwqcxg8ND/+XM3iAviX7FJtpVJi6e+bATeipvbePTDgK2h/xbJGyY0g=="
                                                                }

                                                                {
                                                                "result": [
                                                                {
                                                                "data": [
                                                                {
                                                                "desc": "",
                                                                "id": "",
                                                                "name": "js_test_tag1",
                                                                "tag": ""
                                                                },
                                                                {
                                                                "desc": "",
                                                                "id": "",
                                                                "name": "js_test_tag2",
                                                                "tag": ""
                                                                },
                                                                {
                                                                "desc": "",
                                                                "id": "",
                                                                "name": "js_test_tag3",
                                                                "tag": ""
                                                                }
                                                                ],
                                                                "status": {
                                                                "code": 0,
                                                                "message": "OK"
                                                                },
                                                                "url": "/connector/get/adgrp"
                                                                }
                                                                ]
                                                        }
```

- **To get users:**

```
{
                                                    "method":"exec",
                                                    "params":[
                                                    {
                                                    "data":{
                                                    "adom":"root",
                                                    "connector":"test",
                                                    "server_type":"json",
                                                    "type":"connector",
                                                    "group":"tag1"
                                                    },
                                                    "url":"/connector/get/user"
                                                    }
                                                    ],
                                                    "session":
"3wiI3MoD4JA6Rfj+ue0sqwqcxg8ND/+XM3iAviX7FJtpVJi6e+bATeipvbePTDgK2h/xbJGyY0g=="
                                                    }

                                                    {
                                                    "result": [
                                                    {
                                                    "data": [
                                                    {
                                                    "grpname": "js_test_tag1",
                                                    "ip_addr": "1.1.1.1",
                                                    "ip_addr6": "::-::",
                                                    "name": "",
                                                    "state": 1
                                                    },
                                                    {
                                                    "grpname": "js_test_tag1",
                                                    "ip_addr": "2.2.2.2",
                                                    "ip_addr6": "::-::",
                                                    "name": "",
                                                    "state": 1
                                                    }
                                                    ],
                                                    "status": {
                                                    "code": 0,
                                                    "message": "OK"
                                                    },
                                                    "url": "/connector/get/user"
                                                    }
                                                    ]
                                        }
```

- **To delete users:**

```
{
                                                    "method": "exec",
                                                    "params": [
                                                    {
                                                    "data": {
                                                    "command": "delete",
                                                    "path": "root/test",
```

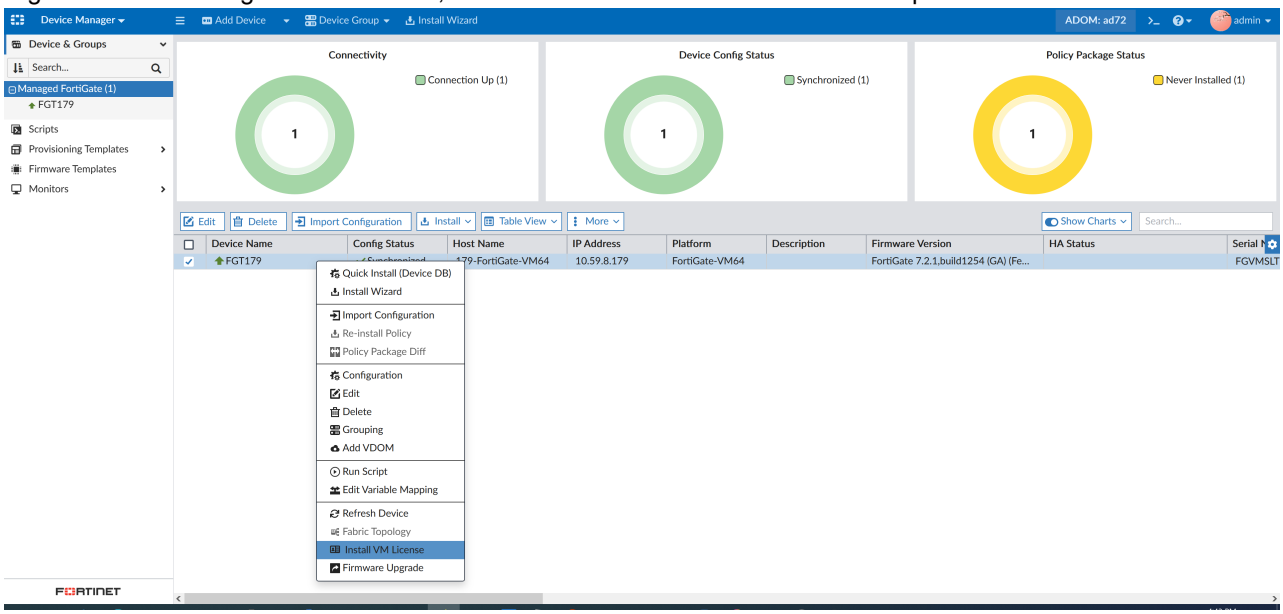
```
                                                    "group": "tag1",
                                                    "ip-addr": [
                                                    "1.1.1.1"
                                                    ]
                                                    },
                                                    "url": "/connector/user/manage"
                                                    }
                                                    ],
                                                    "session":
"3wiI3MoD4JA6Rfj+ue0sqwqcxg8ND/+XM3iAviX7FJtpVJi6e+bATeipvbePTDgK2h/xbJGyY0g=="
                                                    }

                                                    {
                                                    "result": [
                                                    {
                                                    "status": {
                                                    "code": 0,
                                                    "message": "OK"
                                                    },
                                                    "url": "/connector/user/manage"
                                                    }
                                                    ]
                                }
```


## FortiManager supports BYOL installation on managed FortiGate VM - 7.2.1

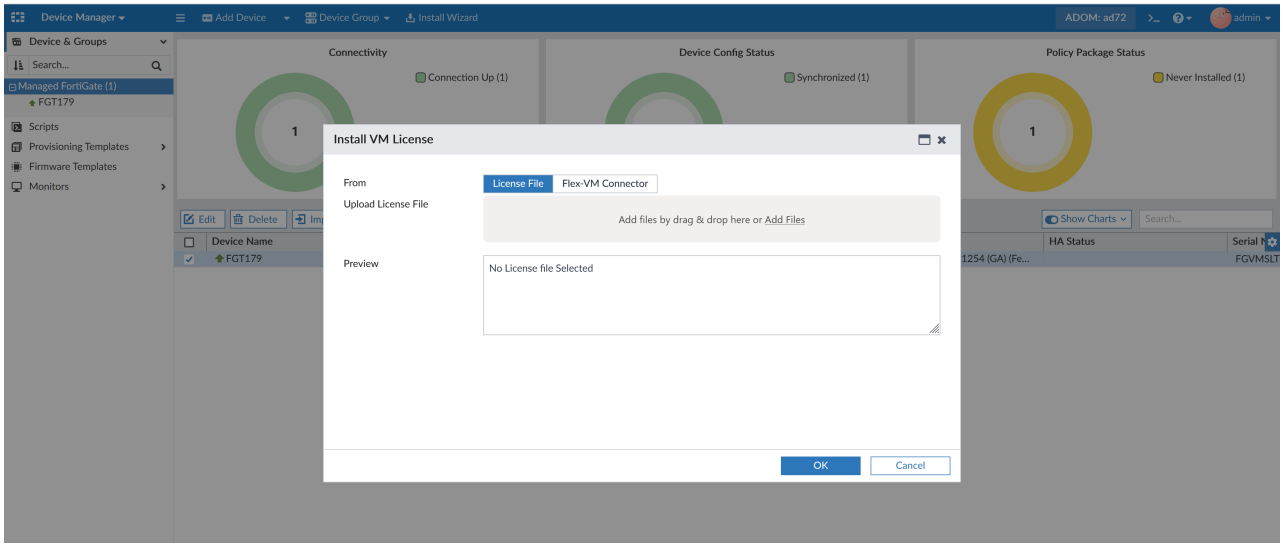
FortiManager supports BYOL installation on managed FortiGate VM.

**To install a BYOL license to a managed FortiGate VM on FortiManager:**

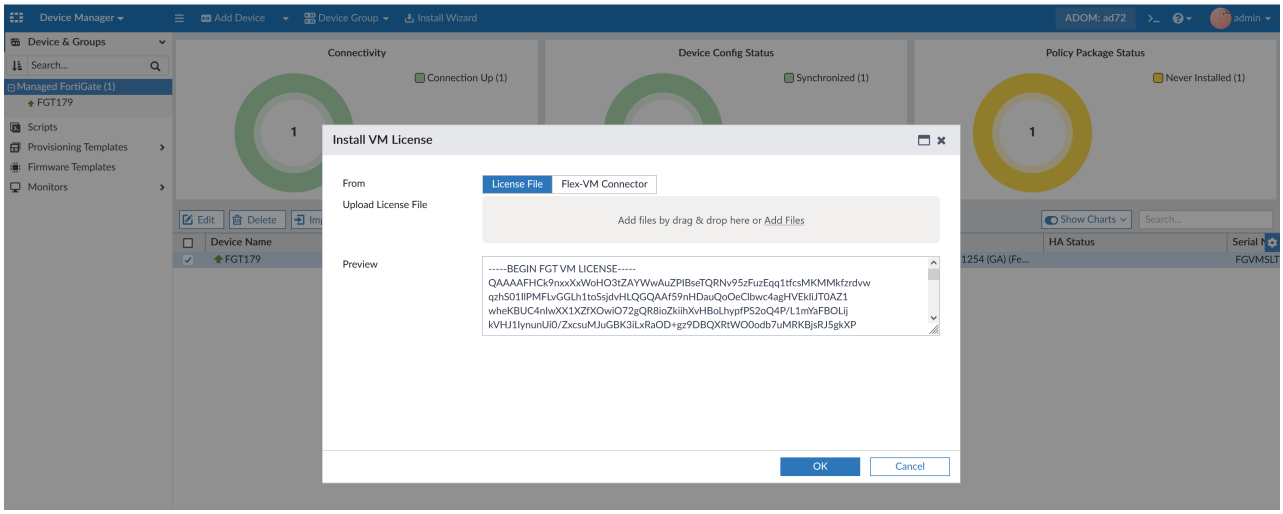
1. Go to *Device Manager* > *Device & Groups*.
2. Right click on a managed FortiGate VM, and select Install VM License from the dropdown menu.



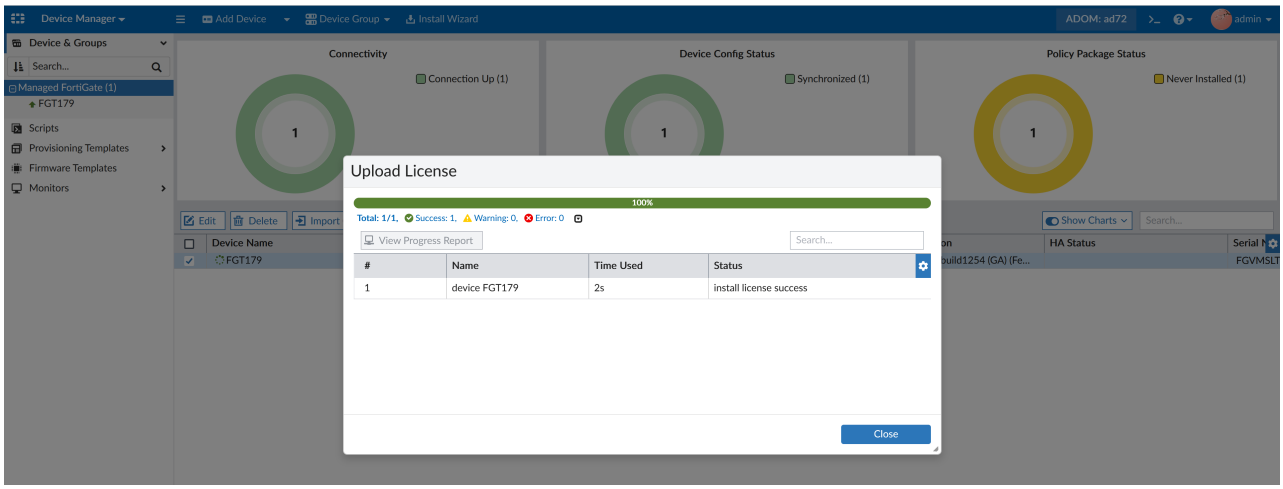
The Install VM License dialog appears with two options for the license: *License File* and *Flex-VM Connector*.

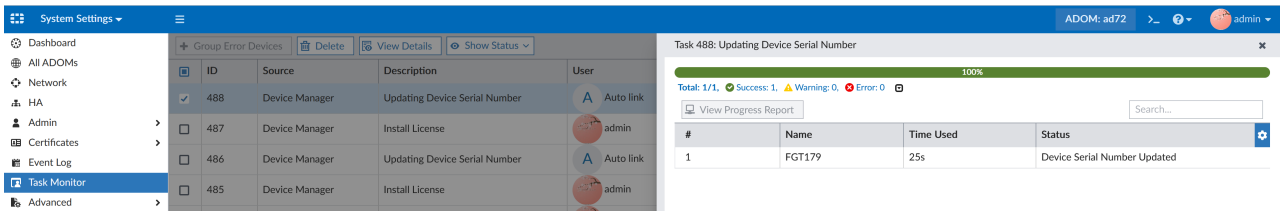



3. Select *License File*, and then upload the license by dragging and dropping the file into the selection box, or clicking *Add Files* to browse to its location.



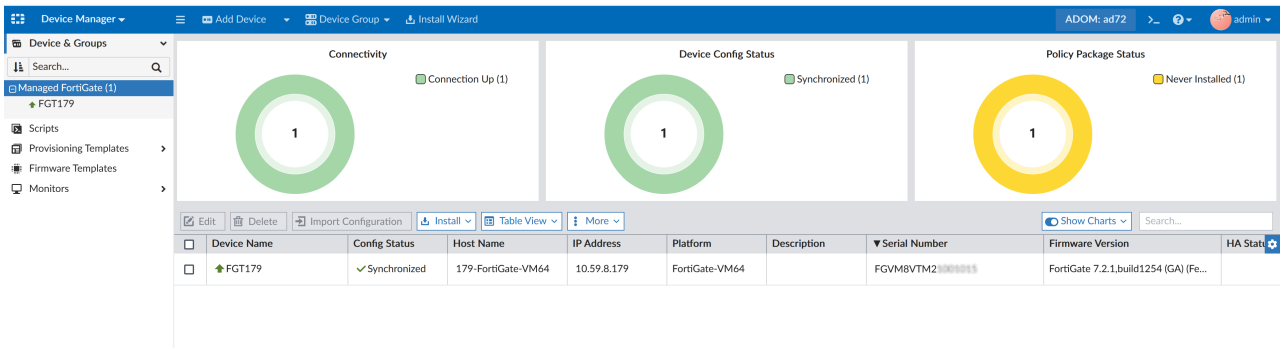

4. Click *OK*.
FortiManager will upload the license and update the Serial Number for the FortiGate device. The FortiGate license is replaced with the new license.




Check the device list, onboard/maintenance member for new the FortiGate serial number.
For example:

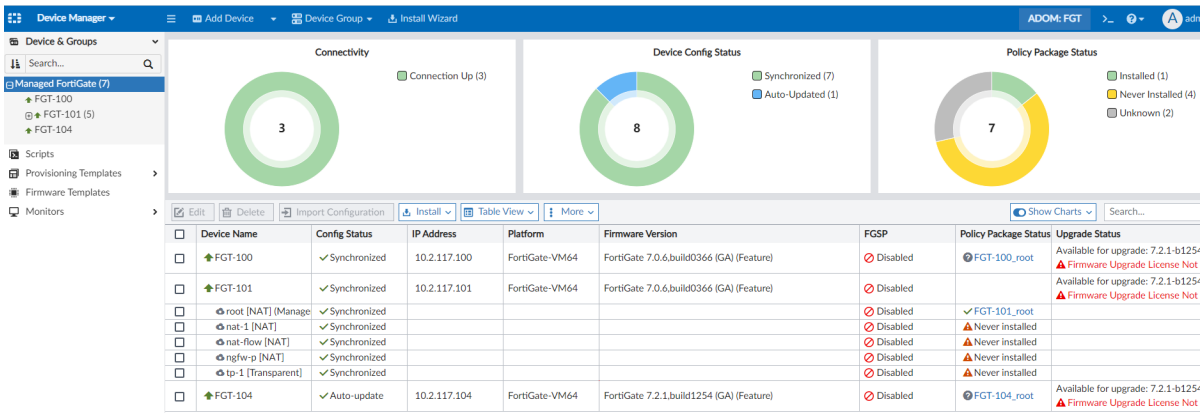
```
diagnose dvm device list FGT179
--- There are currently 49 devices/vdoms managed ---
--- There are currently 42 devices/vdoms count for license ---
TYPE OID SN HA IP NAME ADOM
IPS FIRMWARE
fmgfaz-managed 2267 FGVMSLTM2200001 - 10.59.8.179 179-FortiGate-VM64 ad72
6.00741 (extended) 7.0 MR2 (1254)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
|- vdom:[3]root flags:0 adom:ad72 pkg:[never-installed]
|- onboard/maintenance member:[2279FGVM8VTM21000000
```



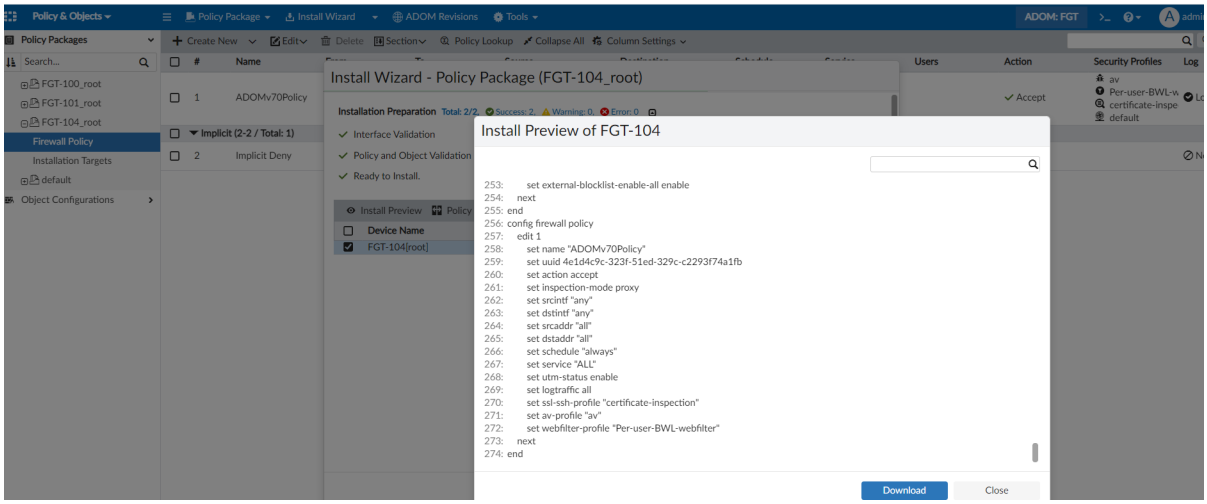

## FortiGates with firmware FOS version 7.0 and version 7.2 can be managed under the same FortiManager 7.0 ADOM - 7.2.1

FortiGates with firmware FOS version 7.0 and version 7.2 can be managed under the same FortiManager 7.0 ADOM.

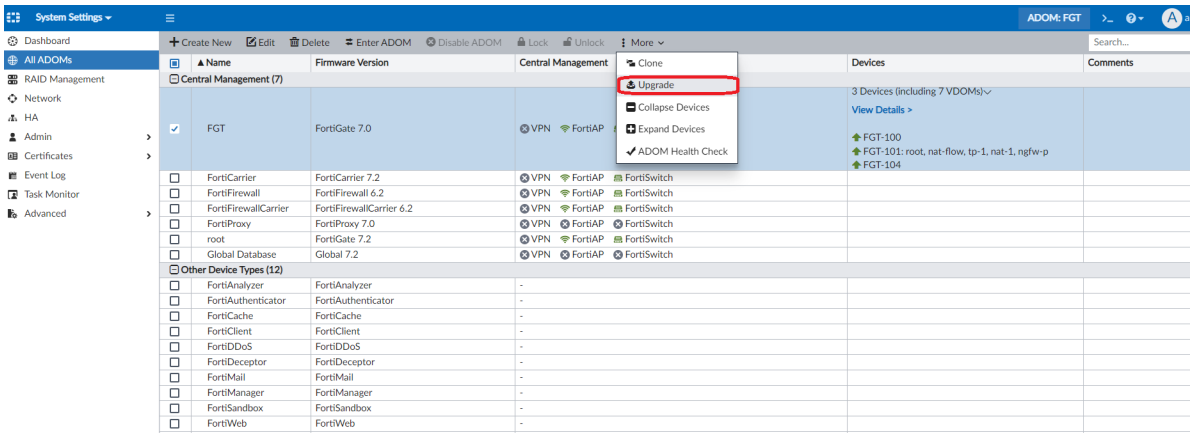
- FortiManager ADOM version 7.0 can manage FortiGate devices on FortiOS 7.0 and 7.2.

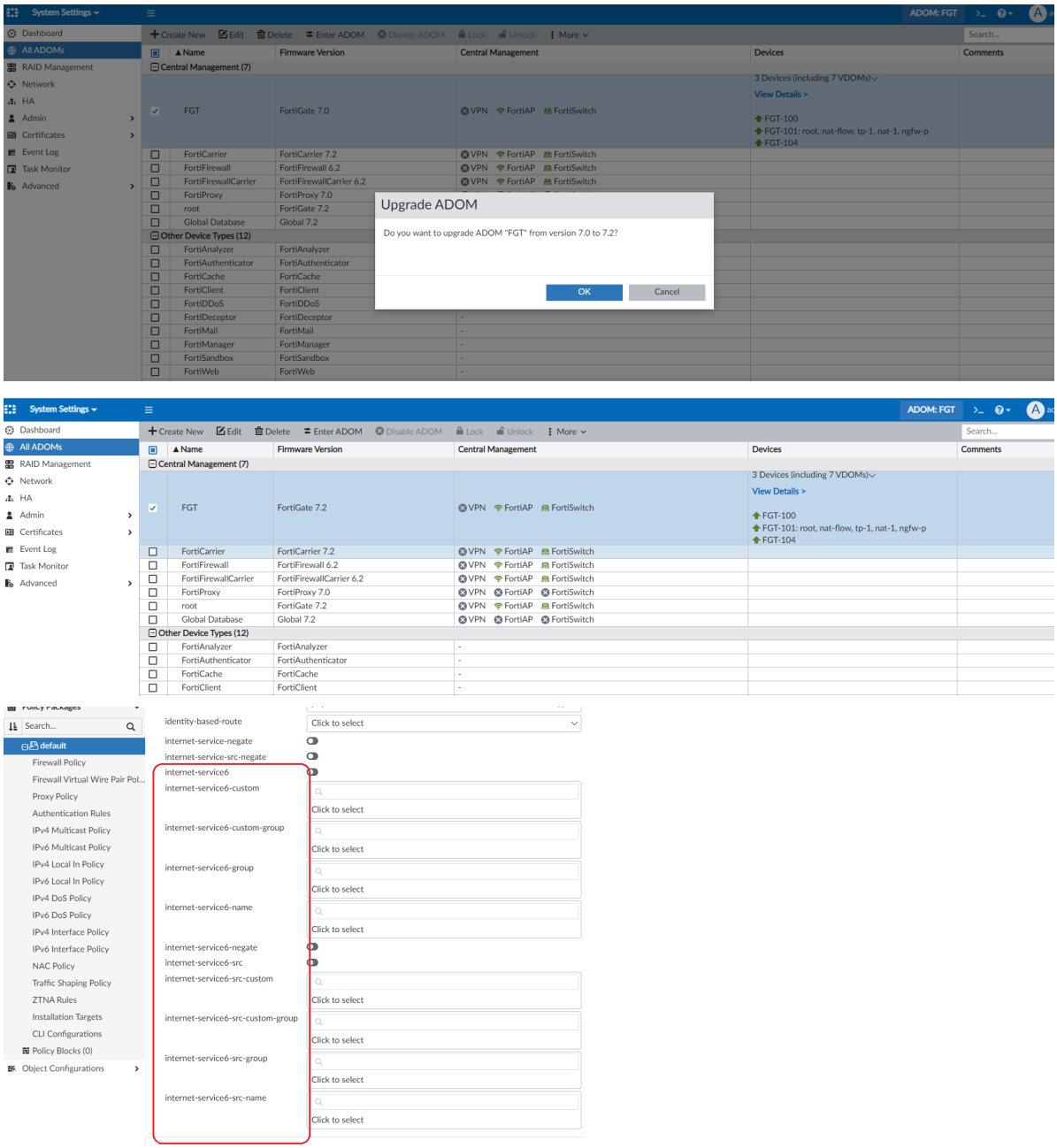



- If an administrator creates a new 7.0 firewall policy in the ADOM and installs it to FortiGate devices on FortiOS 7.2, FortiManager will automatically handle the 7.0 CLI syntax and will not change any of the 7.2 features in the FortiGates.




- Upgrade your ADOM from version 7.0 to 7.2 by navigating to *System Settings* > *All ADOMs*, selecting the 7.0 ADOM, and clicking *More* > *Upgrade*. After the ADOM is upgraded to 7.2, the GUI will automatically display ADOM 7.2 features.

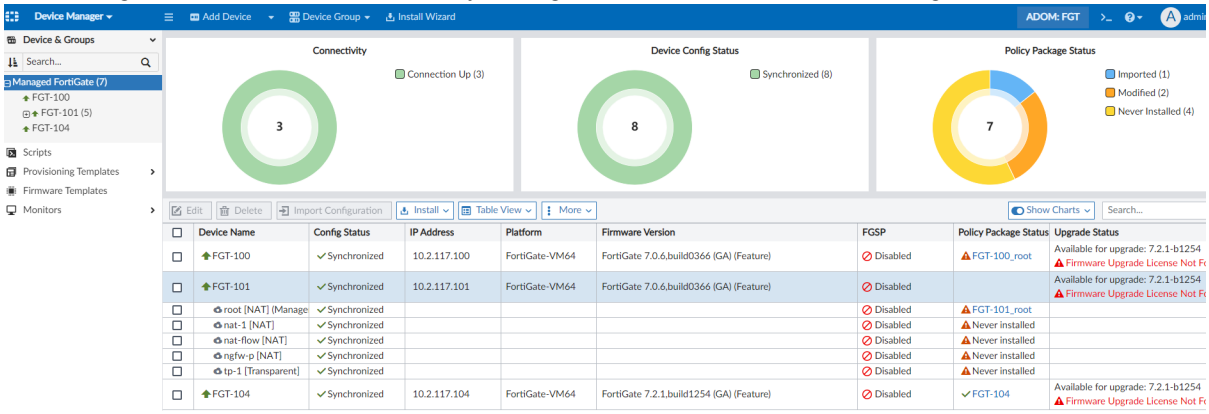




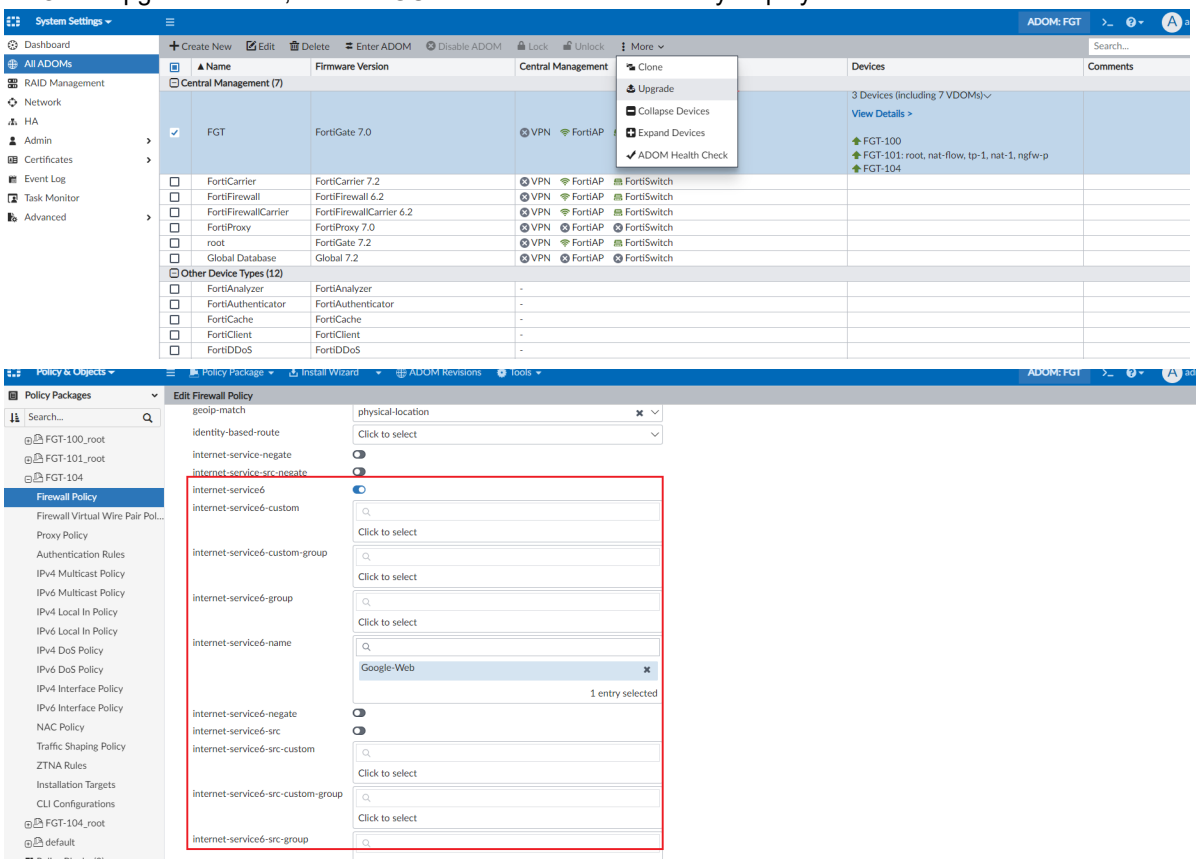

## ADOM version 7.2 supports policy package installation to the lower version of FortiGate on FortiOS 7.0. - 7.2.1

ADOM version 7.2 supports policy package installation to the lower version of FortiGate on FortiOS 7.0. During the installation process the CLI 7.2 syntax is automatically converted to 7.0. syntax to match the OS version.

- FortiManager 7.0 ADOMs can concurrently manage mixed FortiGate devices running FortiOS 7.0 and 7.2.

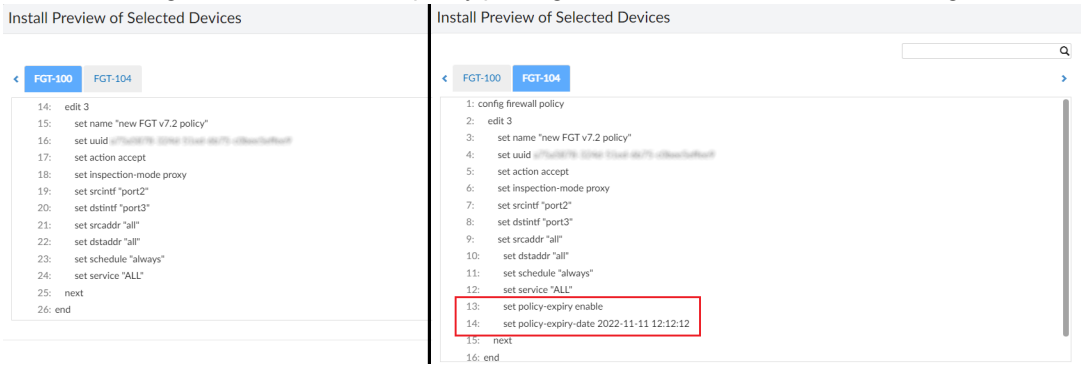



- Navigate to *System Settings* > *All ADOMs* > *More*, and select *Upgrade* to upgrade your 7.0 ADOM to 7.2. After the ADOM is upgraded to 7.2, the new GUI features are automatically displayed.




- In the upgraded 7.2 ADOM, create a new firewall policy and then install the policy to FortiGate units running 7.0 and 7.2. FortiManager will automatically downgrade the 7.2 CLI syntax to 7.0 syntax when the package is installed on

devices running FortiOS 7.0. The full policy package will be installed to devices running FortiOS 7.2.




## Improved FortiSwitch Manager and AP Manager dashboards - 7.2.1

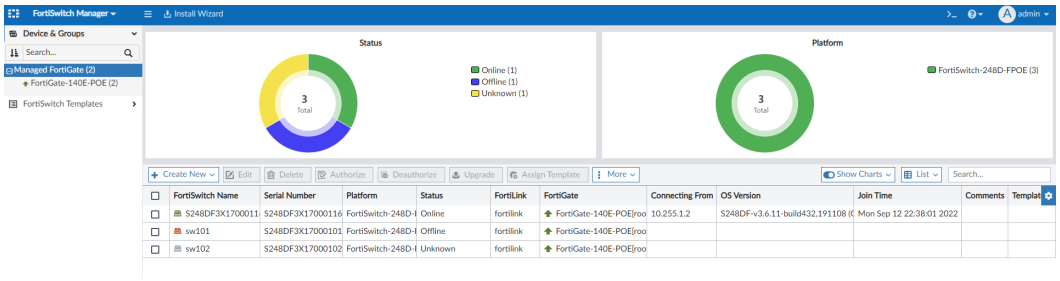
Dashboards are added and improved in *FortiSwitch Manager* and *AP Manager*.

See below for:

- Changes and additions to the FortiSwitch Manager dashboards
- Changes and additions to the AP Manager dashboards

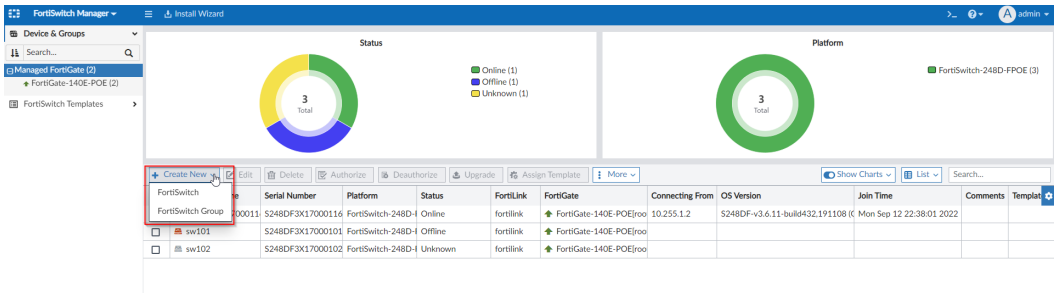
### Changes and additions to the *FortiSwitch Manager* dashboards:

The *Status* and *Platform* charts are added to display a summary. Use the *Show Charts* dropdown and toggle to show or hide the charts. From the *Show Charts* dropdown, you can select or de-select the checkboxes for *Status* and *Platform* to show or hide the respective chart.

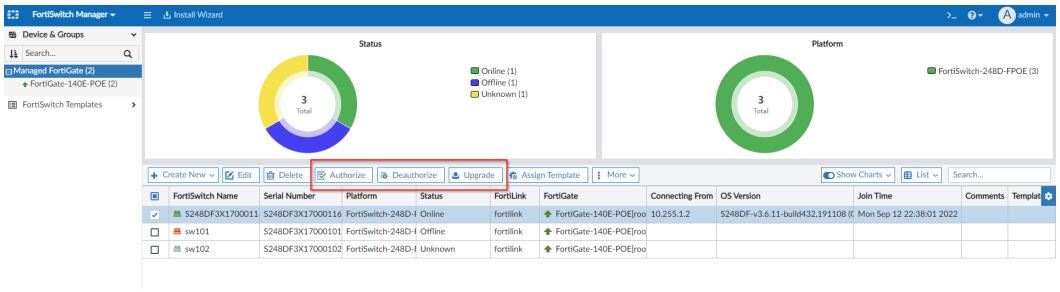



You can mouse over the charts to display a summary of the section in a tooltip. Click an item in a chart or legend to filter the list of FortiSwitch devices by that item. You can click multiple items to apply multiple filters. A filter icon appears next to the chart title to indicate that it is being used to filter the list below. To remove all filters, click the chart title that displays the filter icon.

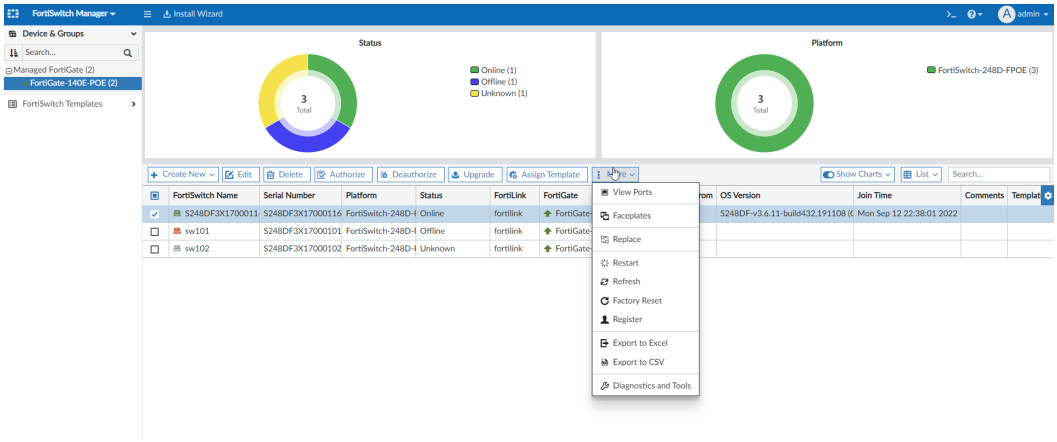
The *Create New* button is replaced with a dropdown. From the *Create New* dropdown, you can add a new *FortiSwitch* or *FortiSwitch Group*.



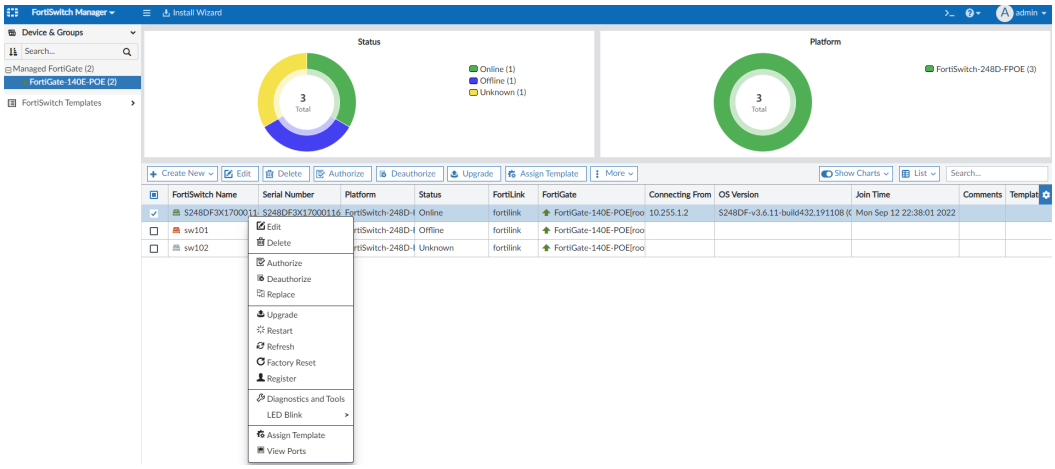

The following options are added to the toolbar to make them more accessible: *Authorize*, *Deauthorize*, and *Upgrade*.



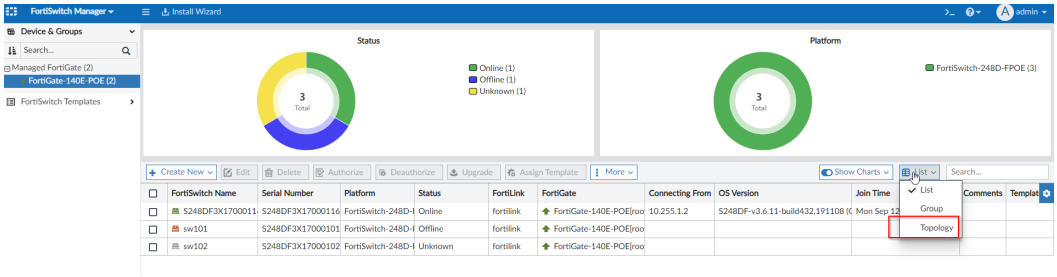

The following options are included in the *More* options dropdown:



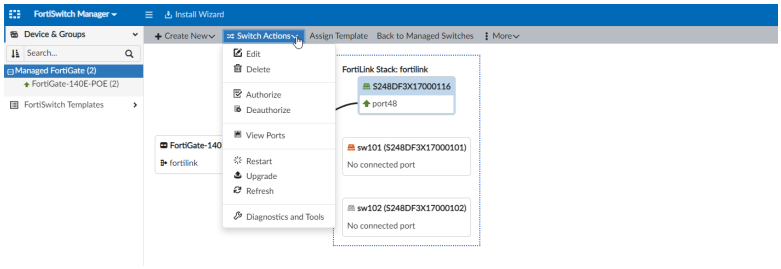

The following options are included in the right-click menu:



The *Topology* monitor is now accessed from the view dropdown.

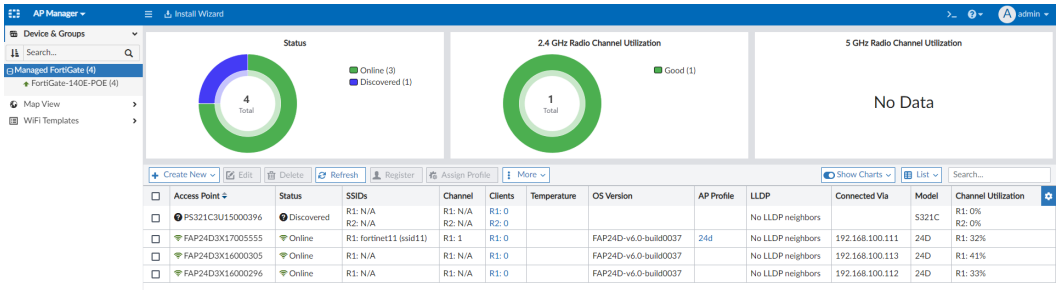



The *Switch Actions* dropdown is added to the toolbar in the *Topology* monitor. To return to the *List* view, click *Back to Managed Switches*.



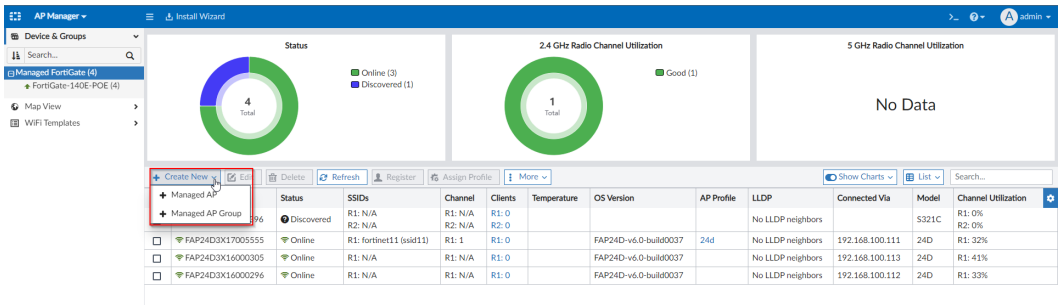

**Changes and additions to the *AP Manager* dashboards:**

The *Status* and *Radio Channel Utilization* dashboards are added to display a summary. Use the *Show Charts* dropdown and toggle to show or hide charts. From the *Show Charts* dropdown, select or de-select checkboxes to show or hide the respective chart.

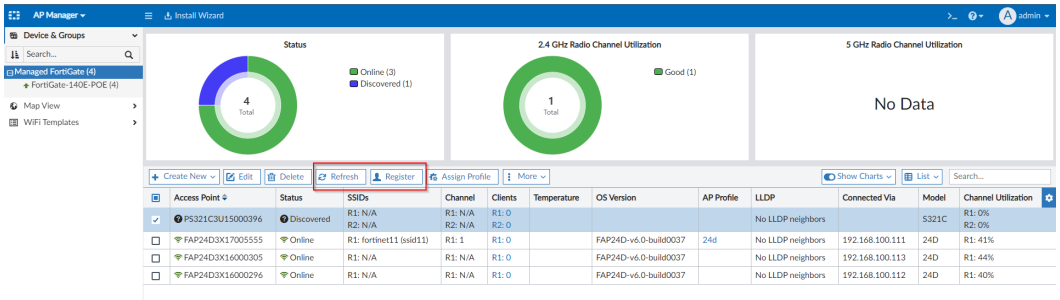



You can mouse over the charts to display a summary of the section in a tooltip. Click an item in a chart or legend to filter the list of FortiSwitch devices by that item. You can click multiple items to apply multiple filters. A filter icon appears next to the chart title to indicate that it is being used to filter the list below. To remove all filters, click the chart title that displays the filter icon.

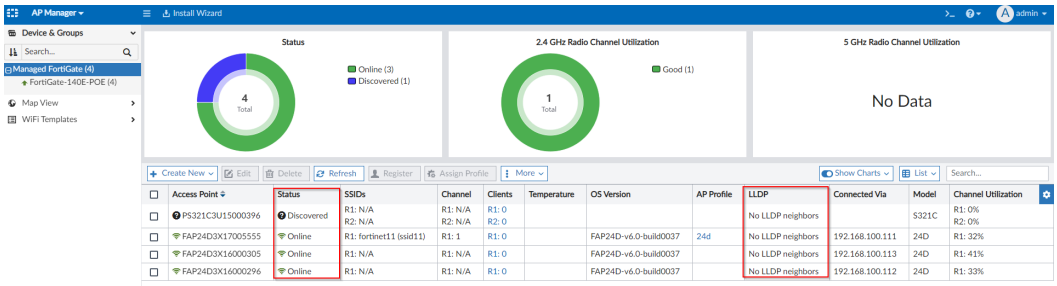
The *Create New* button is replaced with a *Create New* dropdown. From the *Create New* dropdown, you can add a new *Managed AP* or *Managed AP Group*.



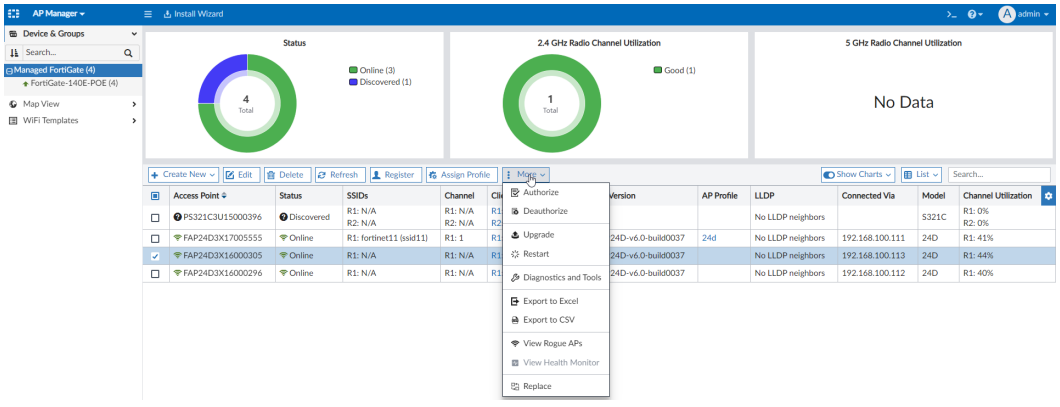

The following options are added to the toolbar to make them more accessible: *Refresh* and *Register*.



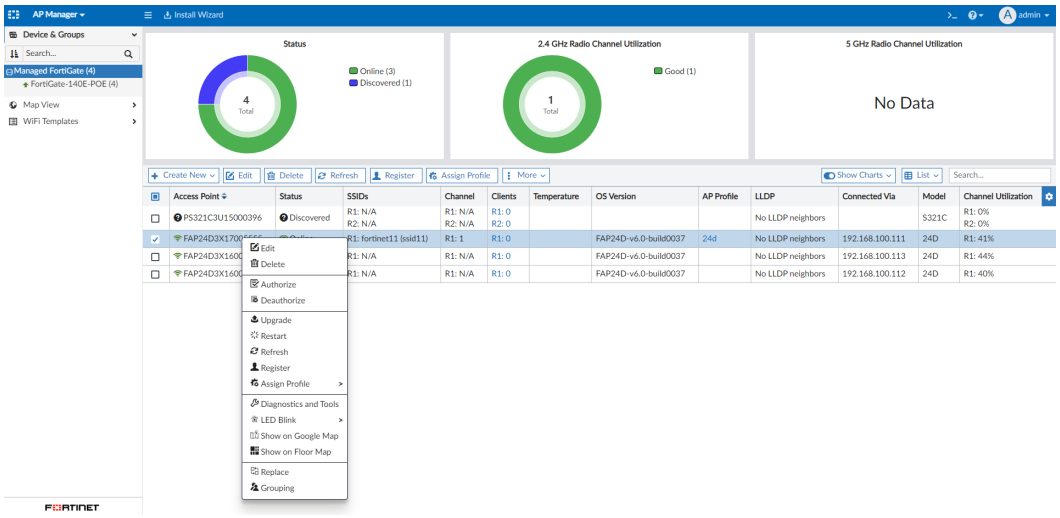

The *Status* and *LLDP* columns are added to the table.



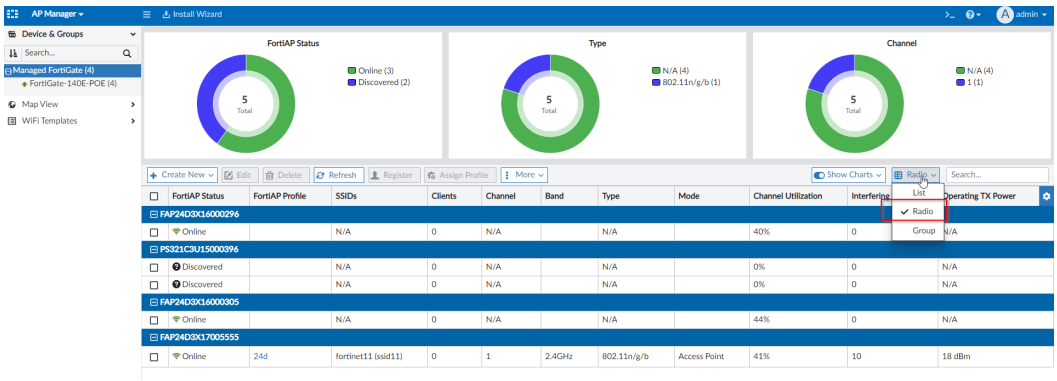

The following options are included in the *More* options dropdown:




The following options are included in the right-click menu:




The *Radio* view is added to the view dropdown. From the view dropdown, you can toggle your view between *List* , *Radio*, and *Group*.




## Option to automatically unlock the ADOM after installing the Policy Package has been added to the Workspace Mode - 7.2.2

The option to automatically unlock the ADOM after installing the Policy Package has been added to the Workspace Mode. This new option can help prevent administrators from accidentally leaving an ADOM locked once they have finished the install.

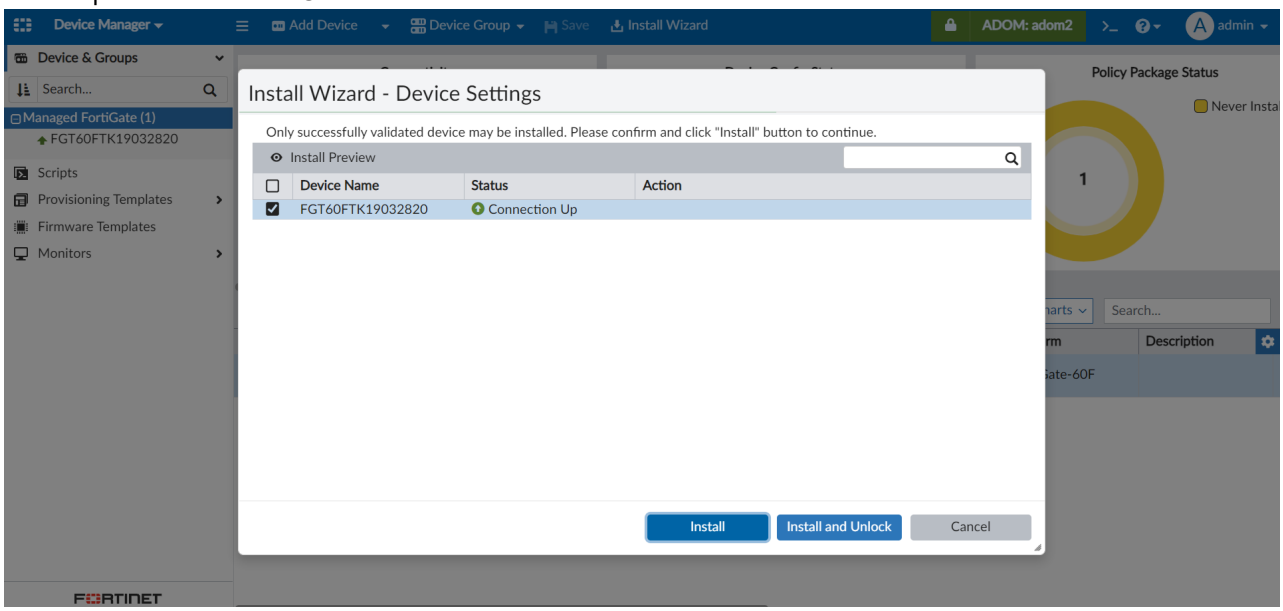
This feature can only be enabled through the CLI

**To enable prompt to unlock ADOM after install:**

1. In the FortiManager CLI, enter the following command to enable the feature.

```
config system global
set workspace-unlock-after-install enable
end
```

2. Enter the ADOM, and perform an install to FortiOS.
   A new option to Install and Unlock is available.



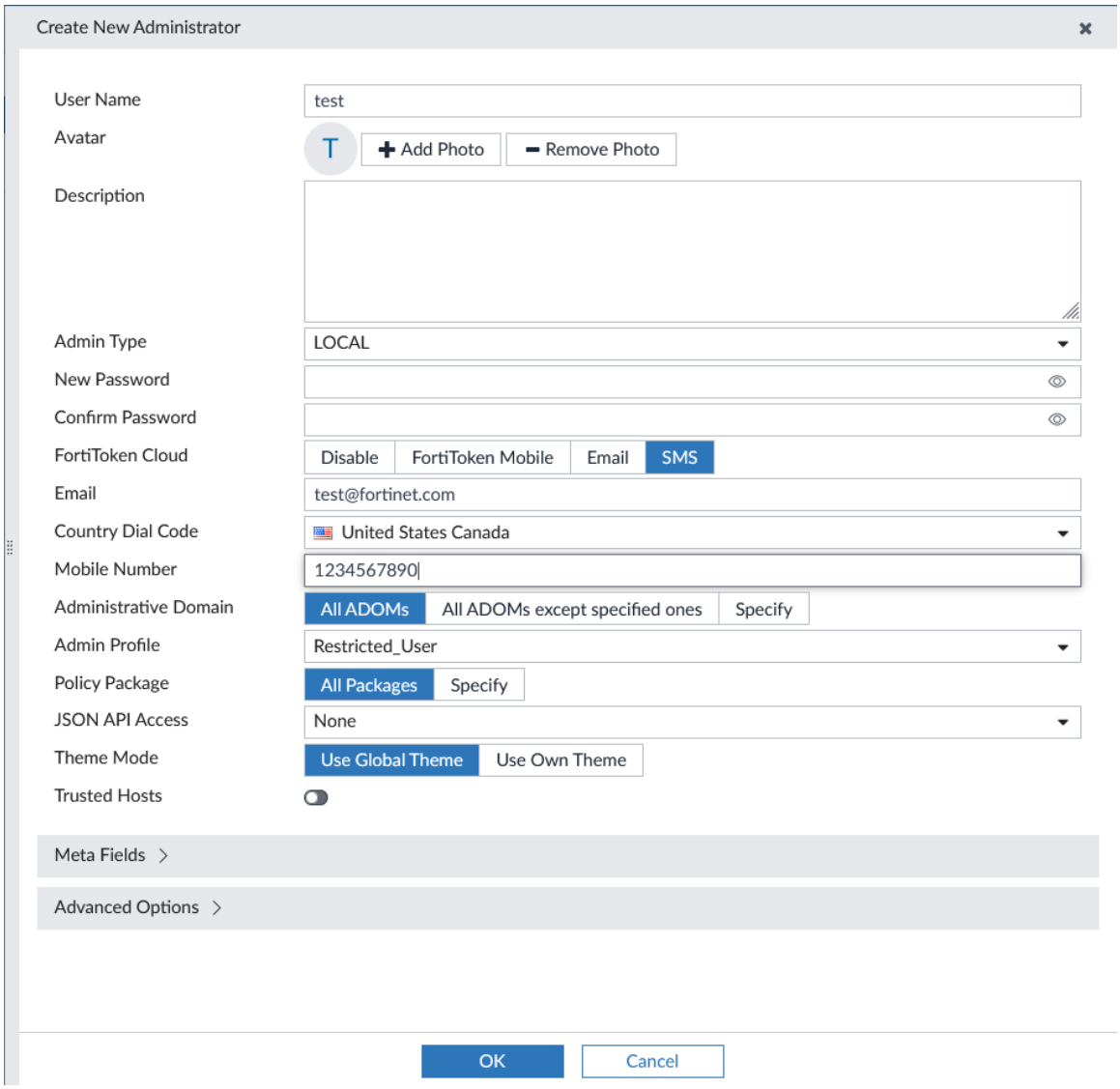

## FortiManager supports 2FA with FortiToken Cloud - 7.2.2

In addition to two-factor authentication (2FA) with FortiAuthenticator for administrator login, FortiManager supports 2FA with FortiToken Cloud.

To use 2FA with FortiToken Cloud, you must have an active FortiToken Cloud license registered on FortiCloud. For more information about this process, see the FortiToken Cloud Admin Guide.

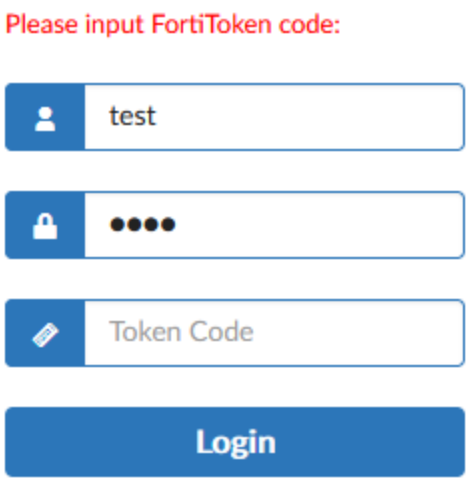
**To configure an administrator to use 2FA with FortiToken Cloud:**

1. In FortiManager, go to *System Settings* > *Admin* > *Administrators* and click *Create New* or edit an existing administrator.
2. In the *FortiToken Cloud* field, select the token delivery method from the following options:
   - *FortiToken Mobile*: Use the FortiToken Mobile app to get tokens. The administrator is sent an email with a link to activate their token in the FortiToken Mobile app on their mobile device.
   - *Email*: Receive the token by email.
   - *SMS*: Receive the token by SMS message.




3. Enter the appropriate contact information.
4. Edit other fields as needed and click *OK*.

   When the administrator logs in, they are prompted to enter the token code from their email, SMS, or FortiToken Mobile.




## Wildcard admin user is supported in the per-ADOM admin profile - 7.2.2

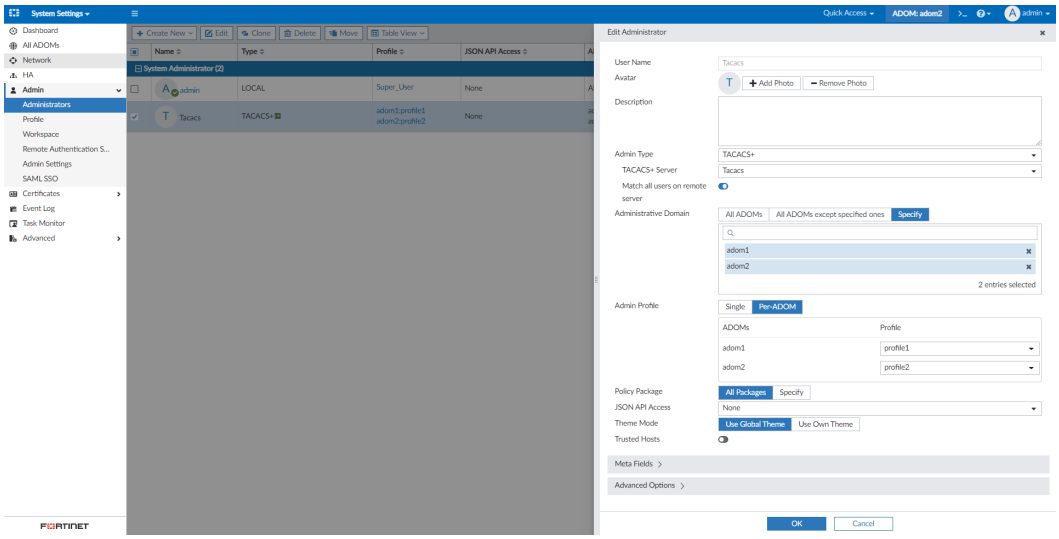
Wildcard admin users now support per-ADOM admin profiles with a profile override option. For more information about the per-ADOM admin profile feature, see Per-ADOM admin profile 7.2.1 on page 218

Additionally, there is a profile override option to use the ADOMs and admin profiles configured on the remote authentication server, if needed.

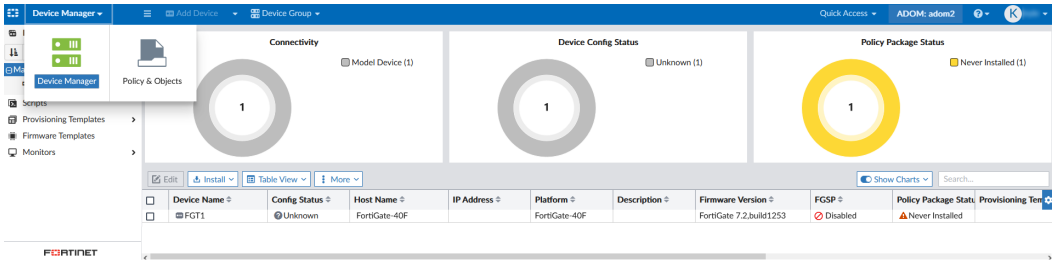
**To configure a wildcard user with the per-ADOM admin profile feature:**

1. Go to *System Settings* > *Admin* > *Administrators*, and click *Create New*.
   You can also edit an existing user to configure per-ADOM access.
2. Select the *Admin Type*, authentication server, and enable *Match all users on remote server* to create a wildcard user.
3. For *Administrative Domain*, specify the ADOMs the users will be able to access.
4. For *Admin Profile*, select *Per-ADOM*.
5. Using the *Profile* dropdowns, select an admin profile for each ADOM.
   The profile determines the administrator's access to the FortiManager features when they are in that ADOM.

In the example pictured below, a TACACS+ wildcard user is configured. However, the same steps can be used to configure another style of wildcard user.



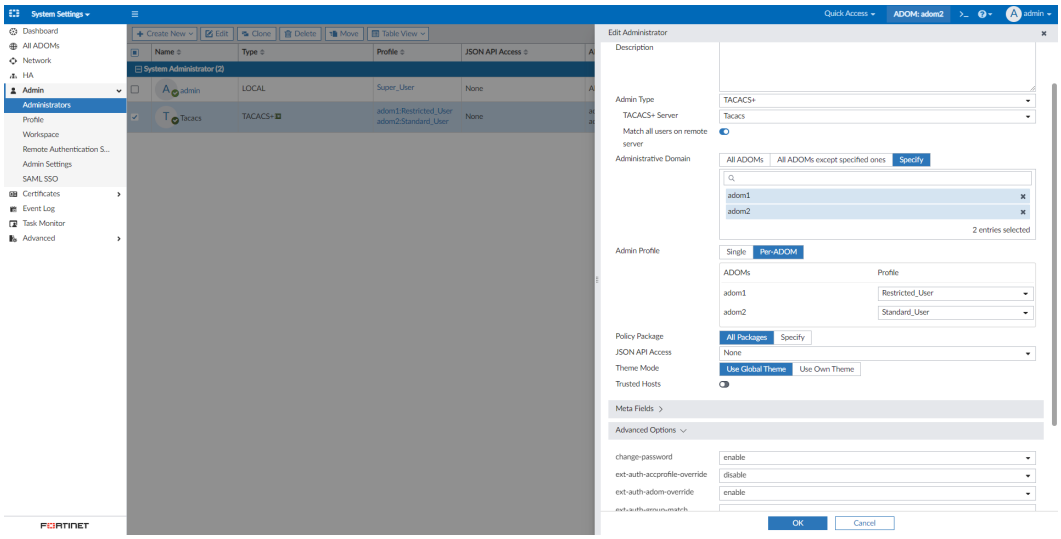

For this example, users logging in as a TACACS+ user will have profile1 access in adom1 and profile2 access in adom2. While profile1 is configured with read-write access across all FortiManager's features, profile2 is limited to *Device Manager* and *Policy & Objects*.



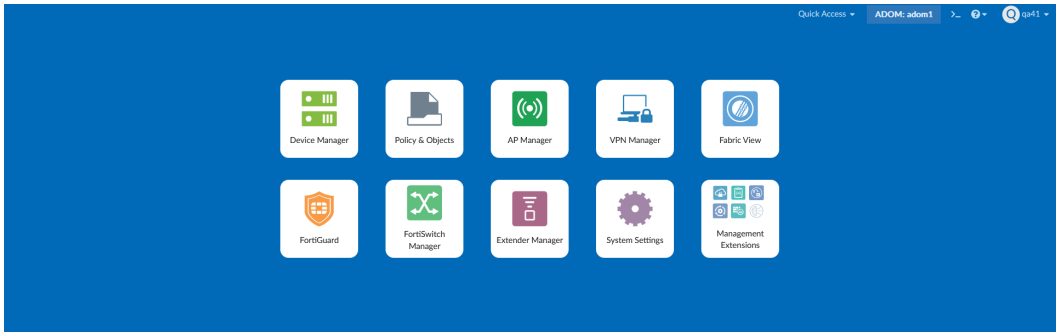

**To use the override feature for wildcard users with per-ADOM profiles:**

1. Configure per-ADOM access on the remote authentication server.
   In this example, the user is configured on the TACACS+ server with profile1 access in adom1 and profile2 access in adom2. Same as above, profile1 is configured with read-write access across all FortiManager's features, and profile2 is limited to *Device Manager* and *Policy & Objects*.
2. Configure the wildcard user.
   In this example, the wildcard user has a per-ADOM configuration with Restricted_User access in adom1 and Standard_User access in adom2. See image below.

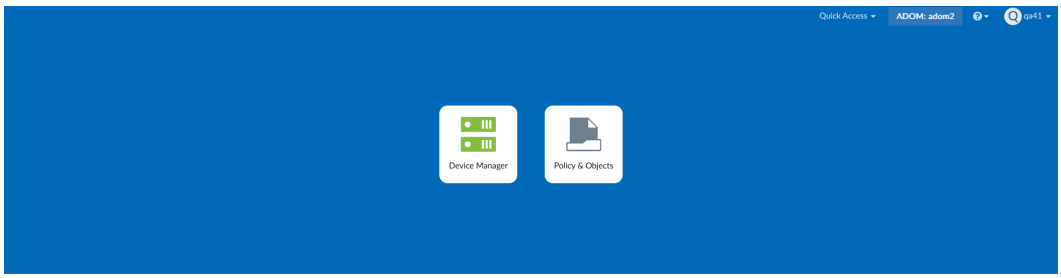
3. In the *Advanced Options* for the wildcard user, enable *ext-auth-adom-override*.




Because the *ext-auth-adom-override* feature is enabled, users logging in as a TACACS+ user will have the per-ADOM access configured on the TACACS+ server. Instead of Restricted_User access in adom1, they will have profile1 access in adom1.




Instead of Standard_User access in adom2, they will have profile2 access in adom2.




## FortiManager supports now the FAZ-BD VM and appliance as managed devices - 7.2.2

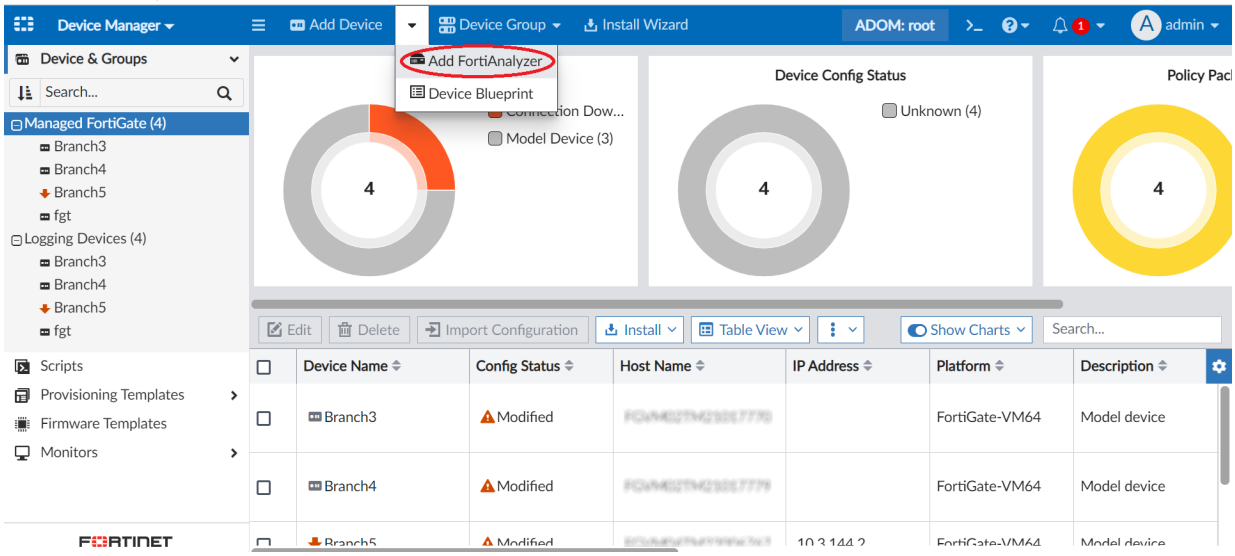
FortiManager supports now the FAZ-BD VM and appliance as managed devices

FortiManager can manage FortiAnalyzer BigData-VM and FortiAnalyzer BigData 4500F models.

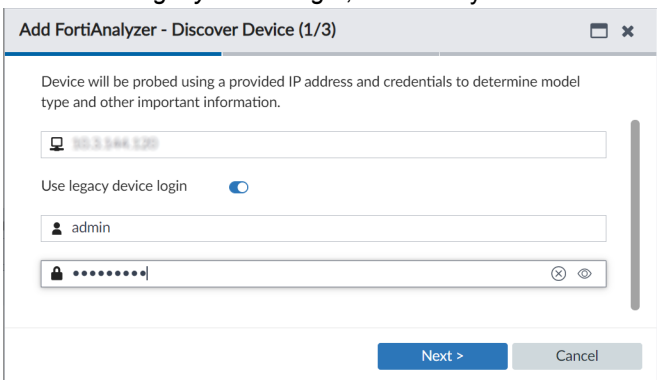
## Managing FortiAnalyzer BigData on FortiManager

### To add FortiAnalyzer BigData to FortiManager:

1. Ensure the *FortiAnalyzer Features* are not enabled in FortiManager.
2. Go to *Device Manager* > *Device & Groups*, and select the dropdown next to the *Add Device* button. Select *Add FortiAnalyzer*.

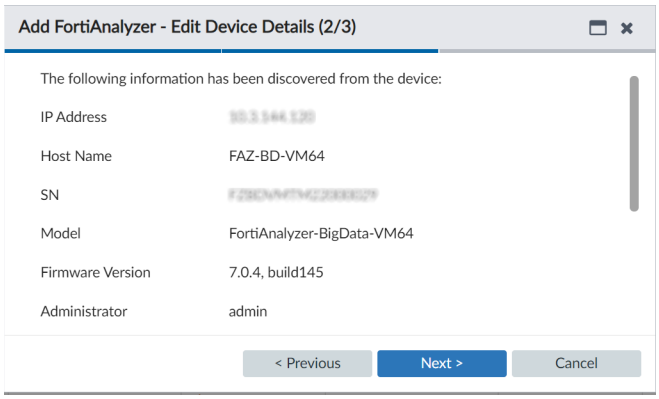



3. Enter the FortiAnalyzer BigData management IP address.
4. Enable *Use legacy device login*, and enter your username and password.



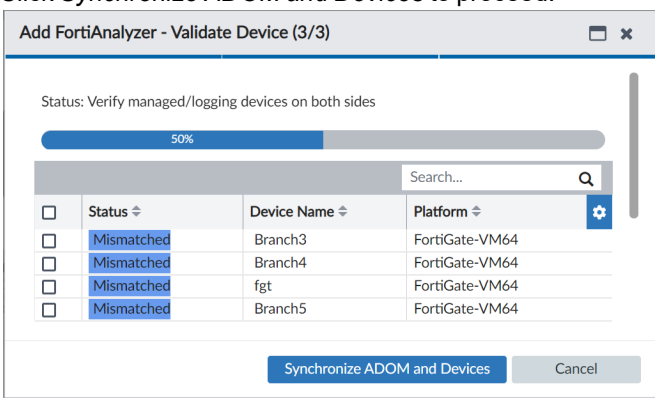

FortiManager will display the basic details of the FortiAnalyzer BigData which will connect to FortiManager.

5. Click *Next*.

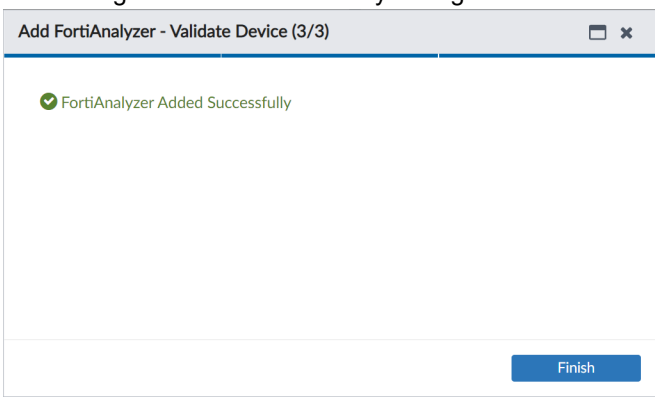



The wizard will ask to synchronize the ADOM and devices.

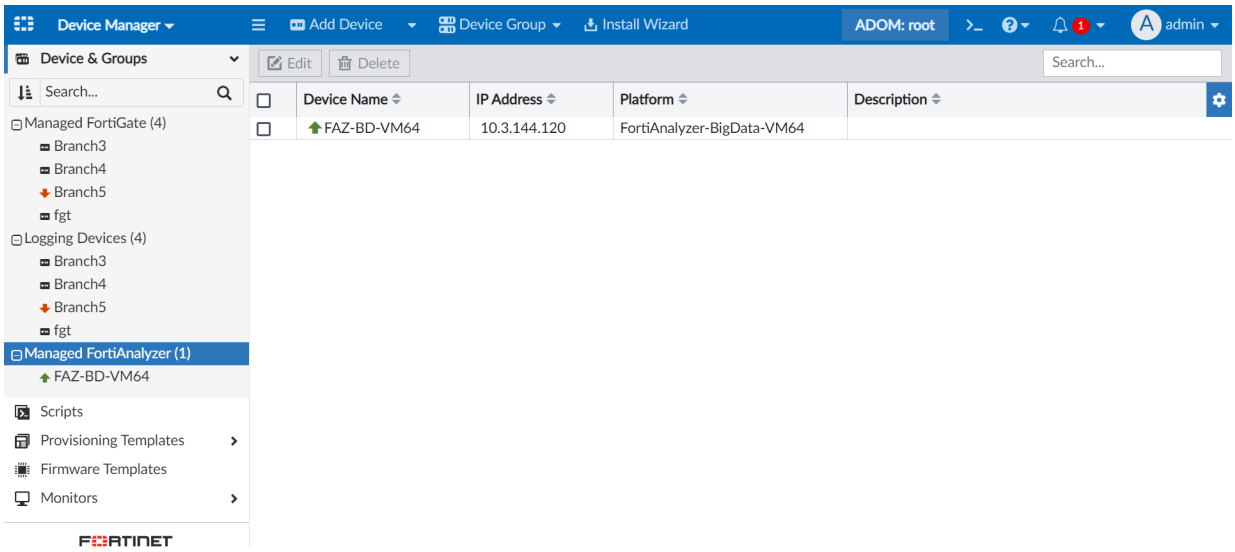
6. Click *Synchronize ADOM and Devices* to proceed.




FortiManager shows the FortiAnalyzer BigData was added successfully.



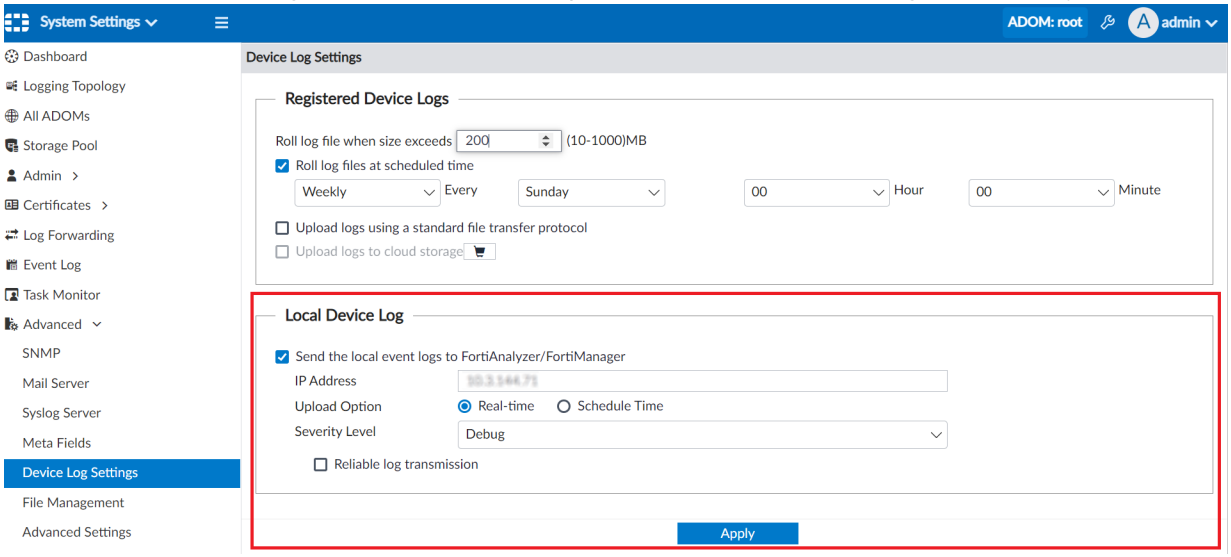

7. To verify that it has connected to FortiManager, go to Device Manager and click Managed FortiAnalyzer. FortiManager will show the version, platform, and IP address of the FortiAnalyzer BigData.


Device Manager
Add Device
Device Group
Install Wizard
ADOM: root
admin
Device & Groups
Search...
Edit
Delete
Search...
Device Name
IP Address
Platform
Description
Managed FortiGate (4)
Branch3
Branch4
Branch5
fgt
Logging Devices (4)
Branch3
Branch4
Branch5
fgt
Managed FortiAnalyzer (1)
FAZ-BD-VM64
FAZ-BD-VM64
10.3.144.120
FortiAnalyzer-BigData-VM64
Scripts
Provisioning Templates
Firmware Templates
Monitors
FORTINET

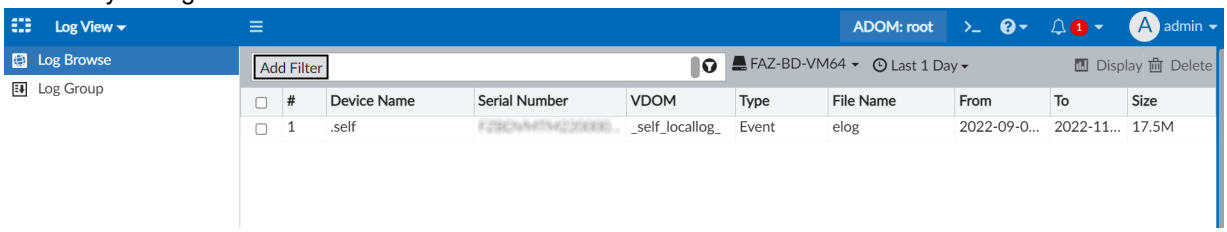
## Sending logs to FortiManager

**To send logs from FortiAnalyzer BigData to FortiManager:**

1. Enable FortiAnalyzer Features on FortiManager.
2. On the FortiAnalyzer BigData go to *System Settings* > *Advanced* > *Device Log Settings*.
3. Go to the *Local Device Log* section and check the option to *Send the local event logs to FortiAnalyzer/FortiManager*.




4. To verify that logs are being sent from FortiAnalyzer BigData, go to *Log View* on the FortiManager and select the FortiAnalyzer BigData device.




## Using FortiManager as the FDS server

This setting can only be configured in the CLI.

**To configure FortiManager as the FDS server for FortiAnalyzer BigData:**

1. Configure FortiManager as the FDS server using the following commands in the FortiAnalyzer BigData CLI:

```
config fmupdate fds-setting
   config server-override
      set status enable
         config servlist
            edit 1
            set ip <FortiManager IP>
            set port 8890
         next
      end
```

```
      end
    end
```

To receive package updates from FortiManager, enter the following commands in the FortiAnalyzer BigData CLI:

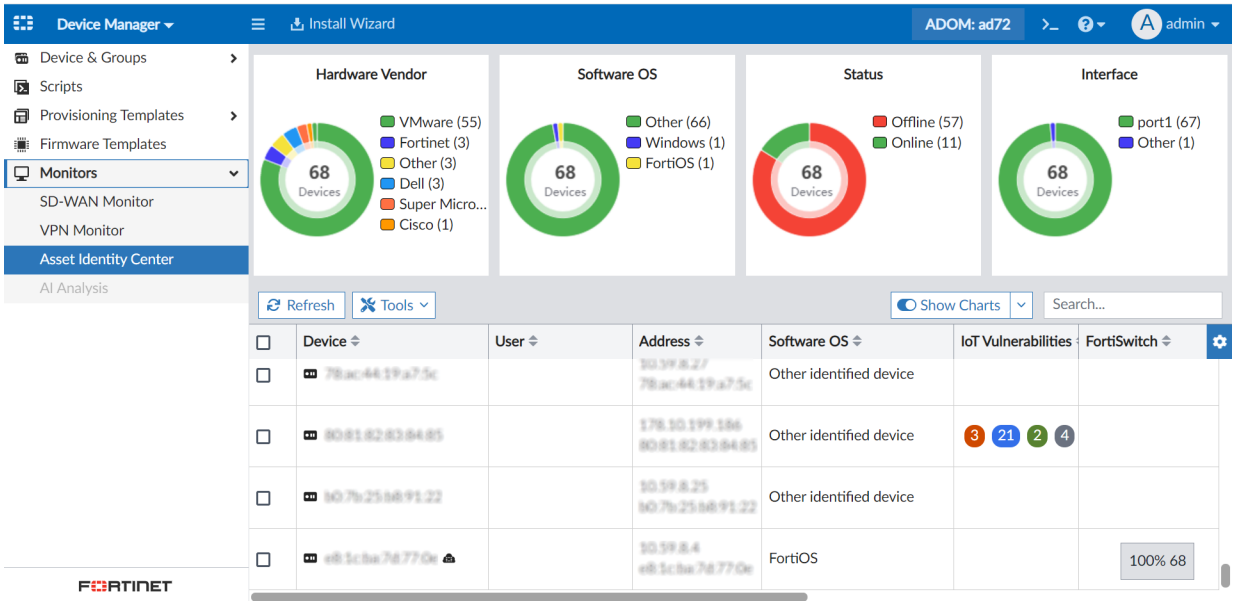
```
fmupdate web-spam fgd-setting
   config server-override
      set status enable
         config servlist
            edit 1
            set ip <FortiManager IP>
            set port 8900
            set service-type fgd
            next
            edit 2
            set ip <FortiManager IP>
            set port 8903
            set service-type geoip
         next
      end
   end
end
```

## IoT Vulnerabilities has been added to the Asset Identity Center - 7.2.2

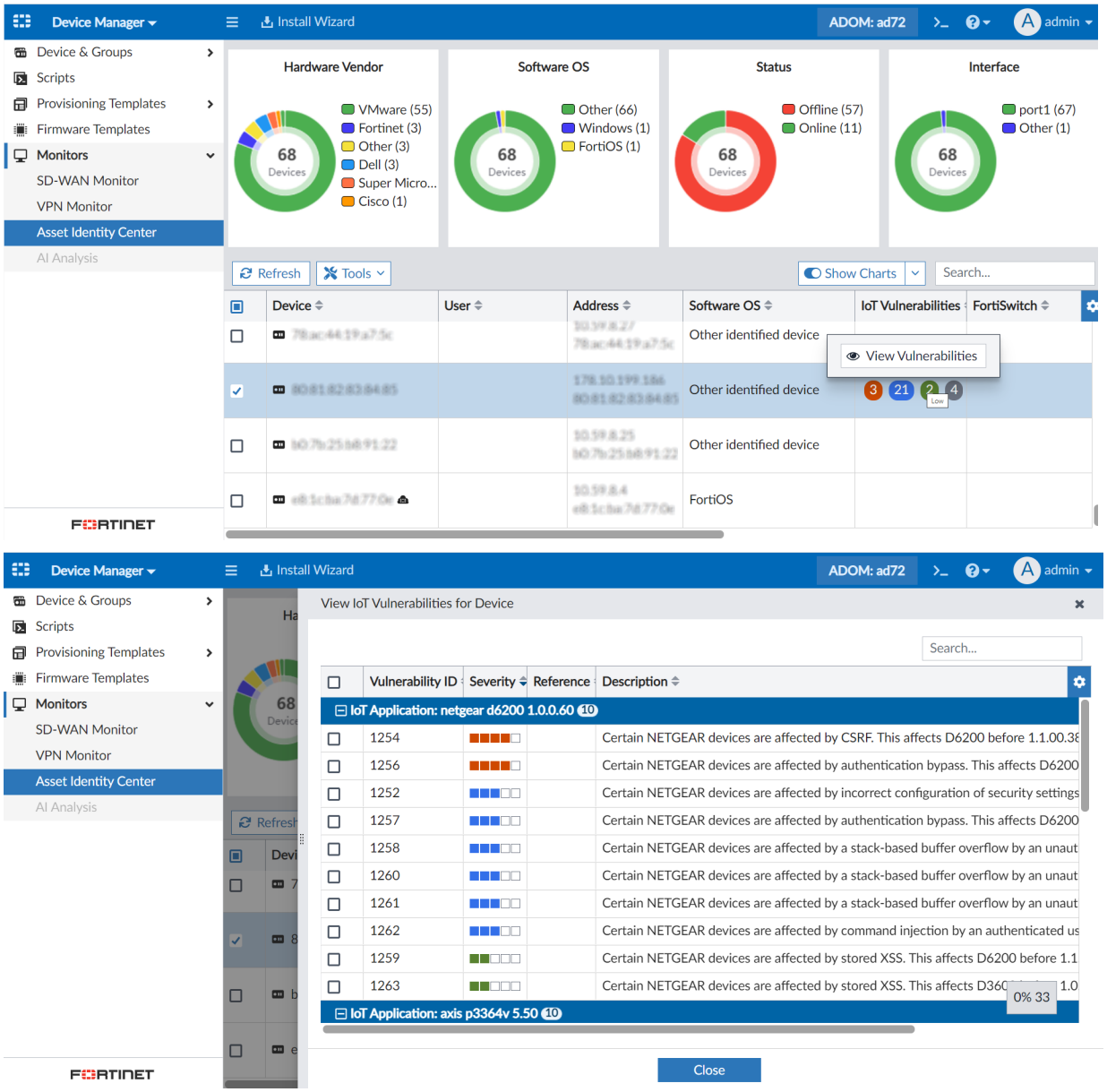
IoT Vulnerabilities has been added to the Asset Identity Center, with the ability to drilldown to the device level to display vulnerability details for each affected device.

**To view IoT vulnerability information:**

1. Go to *Device Manager* > *Monitors* > *Asset Identity Center*.
   The GUI displays the *IoT Vulnerability* information column in the table.



2. Click on the information in the *IoT Vulnerability* column to view vulnerability details.

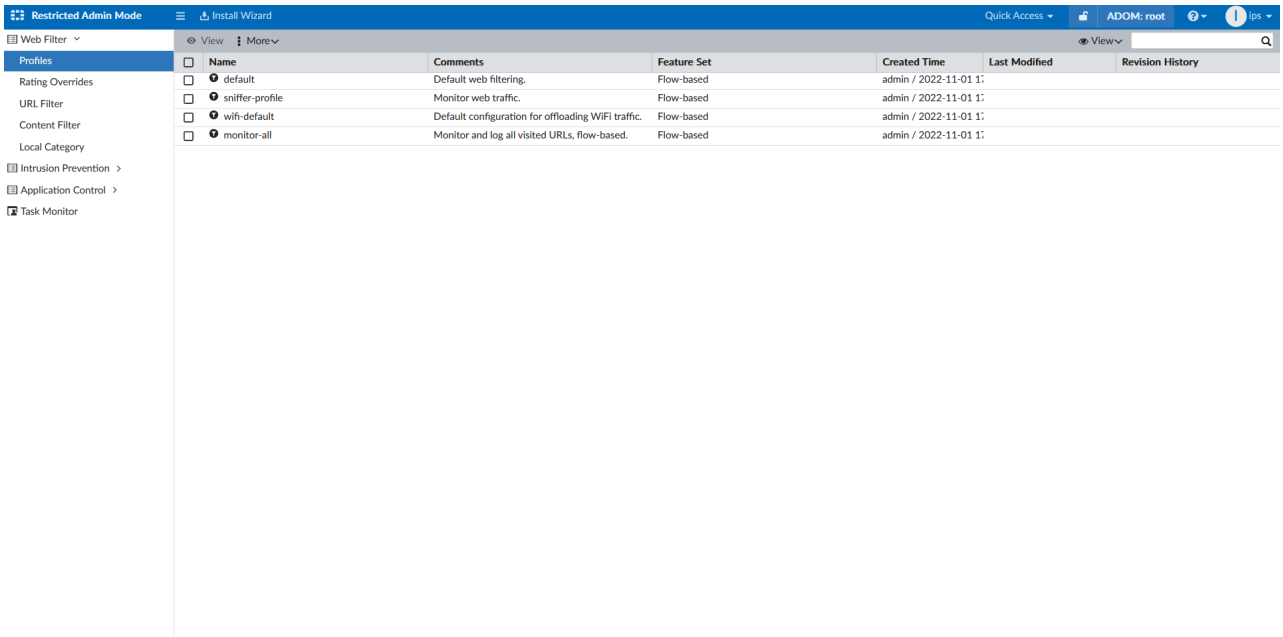



## Workspace mode is supported for the restricted admin - 7.2.2

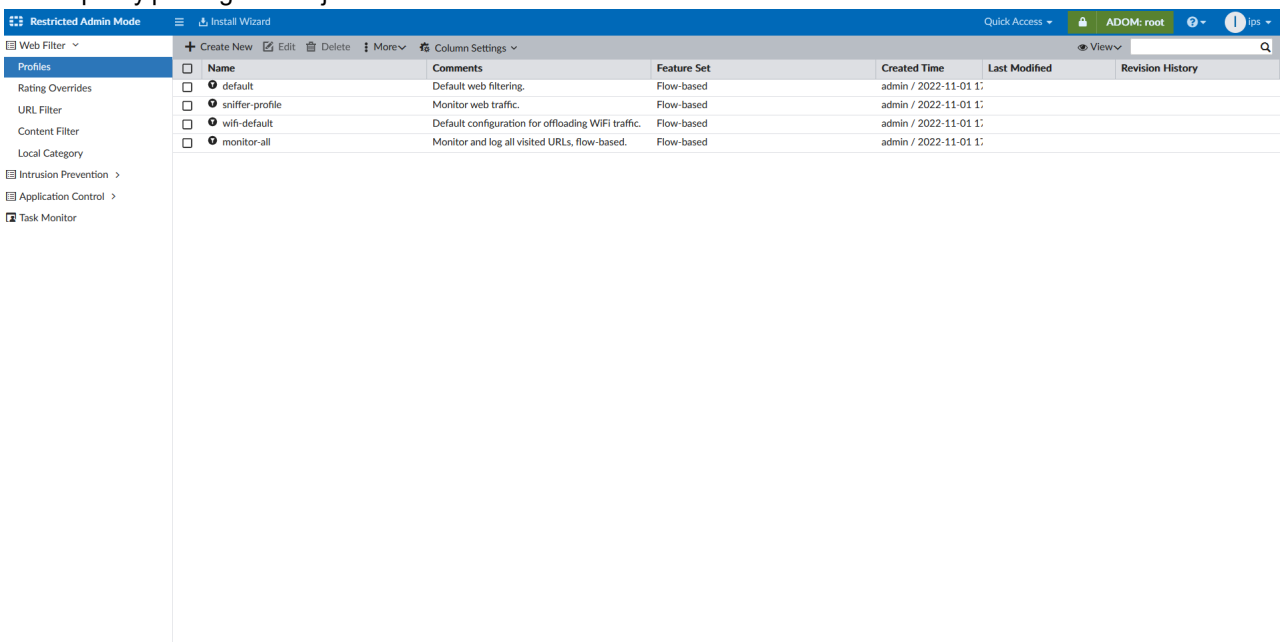
Workspace mode is supported for the restricted admin.

**To use workspace mode as a restricted admin:**

1. Log in as a restricted administrator.
   When Workspace mode is enabled, a lock icon is displayed in the top right. When the lock icon is not displayed, the restricted administrator only has read access to profiles.

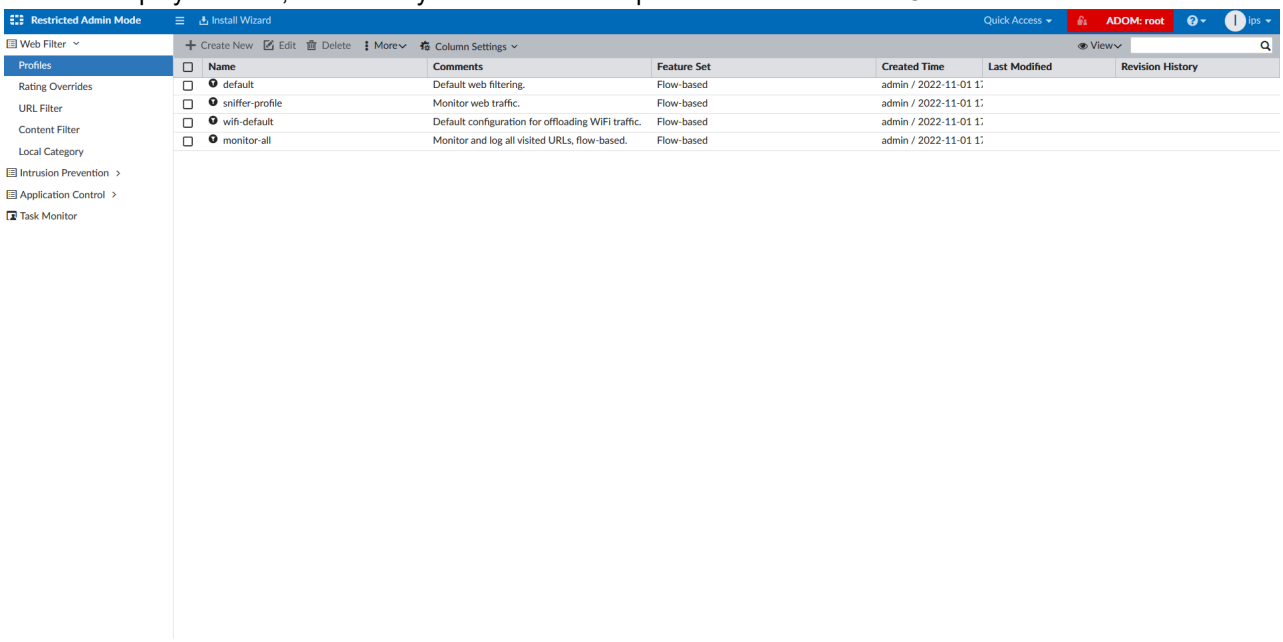



2. Click the lock icon to lock the ADOM. When the ADOM is locked, you are able to create, edit, and delete profiles. Locking the ADOM as a restricted admin user does not lock the whole ADOM, and local administrators are still able to lock policy packages or objects.




When a local administrator locks the ADOM, the whole ADOM is locked. Restricted admin users are able to see the

lock icon displayed in red, and will only have read access permissions until the ADOM is unlocked.

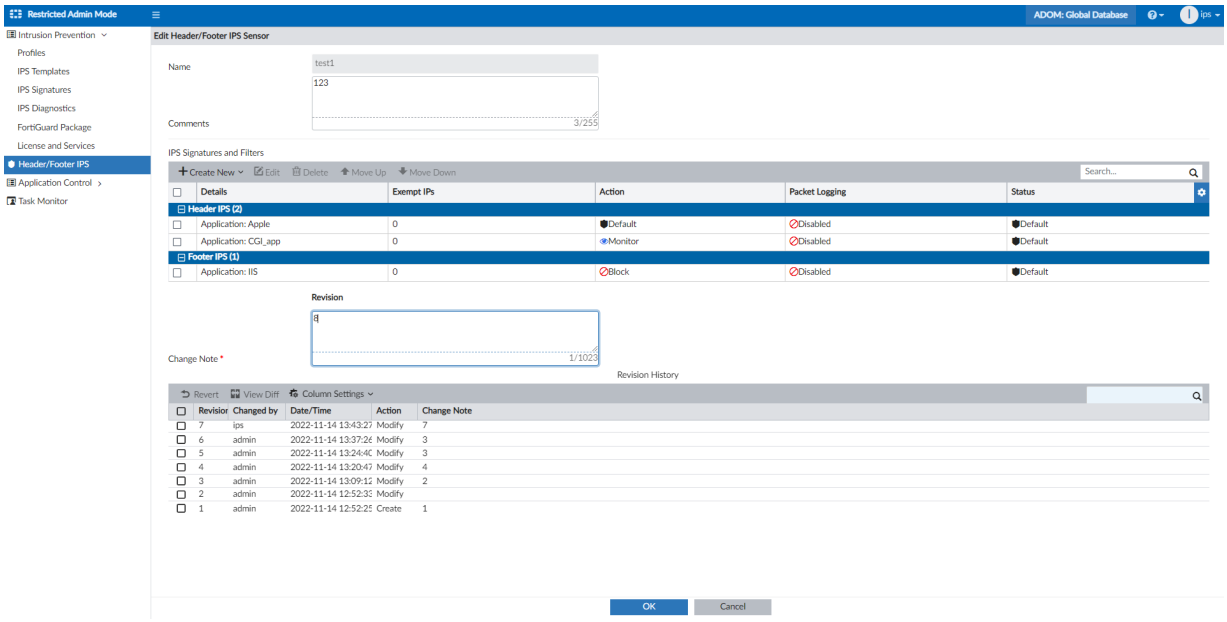



## Restricted IPS admins can manage the IPS header and footer and perform IPS installations in the global ADOM - 7.2.2

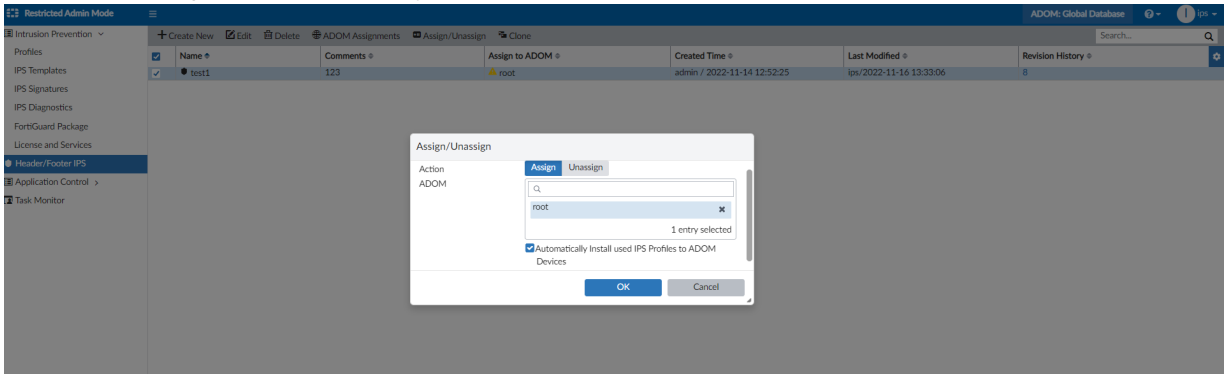
Restricted IPS admins can manage the IPS headers and footers and perform IPS installations in the global ADOM.

**To manage IPS headers and footers in the global ADOM:**

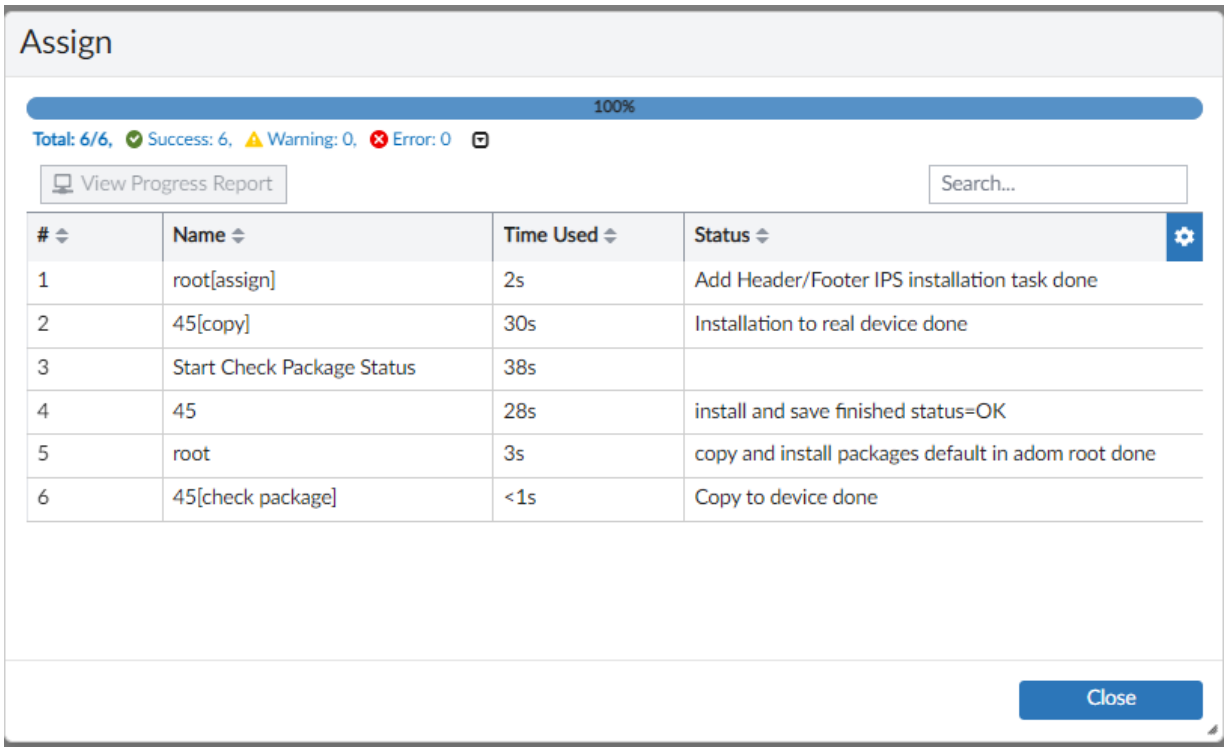
1. Sign in to FortiManager as a restricted IPS administrator.
2. Go to the Global Database ADOM.
   - Restricted IPS admins can create, modify, and operate global IPS header and footers from the Global Database ADOM when managing IPS.



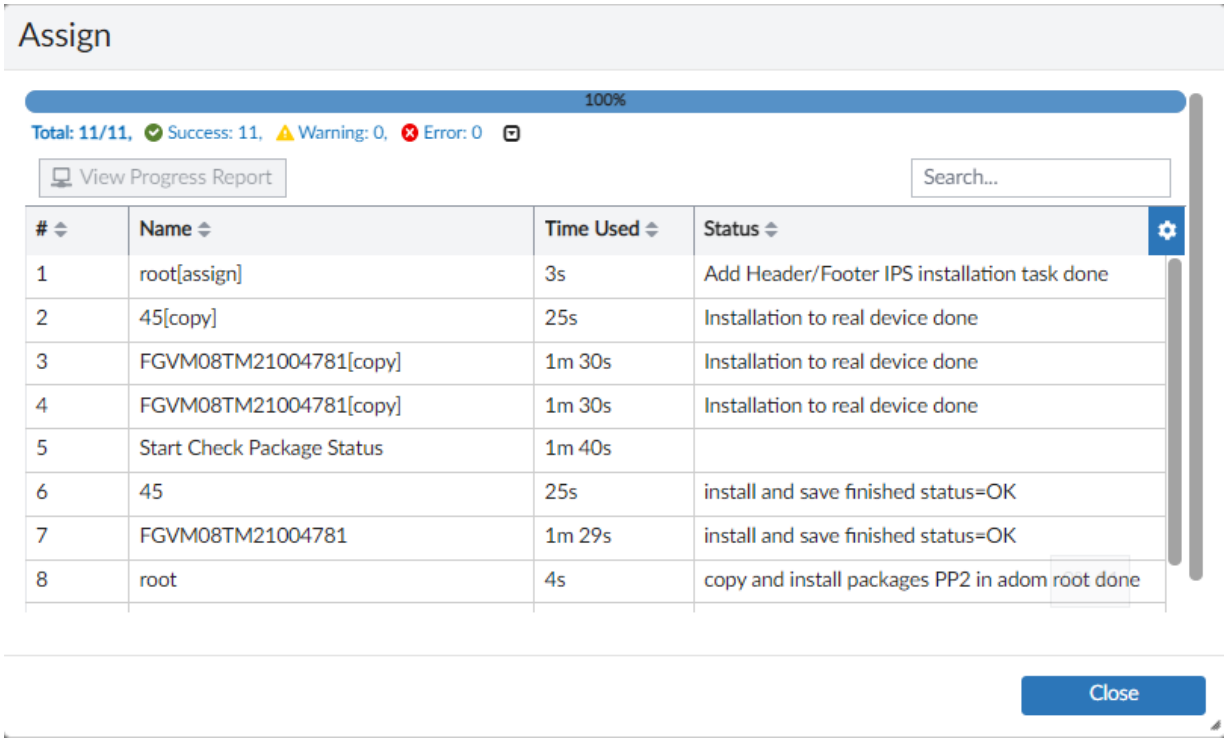

- Users have the option to *Automatically Install Used IPS Profiles to ADOM Devices*.



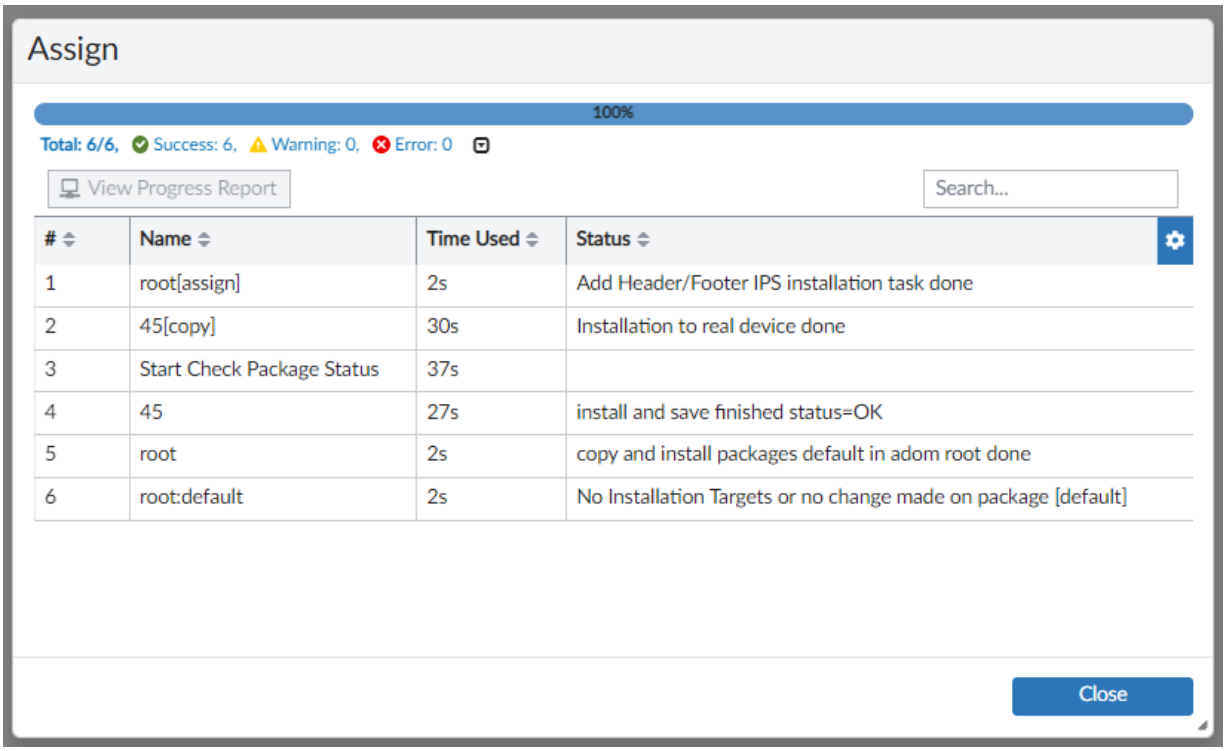
- The following example shows the automatic install to one device in one policy package.




- The following example shows the automatic install to multiple devices in multiple policy packages.



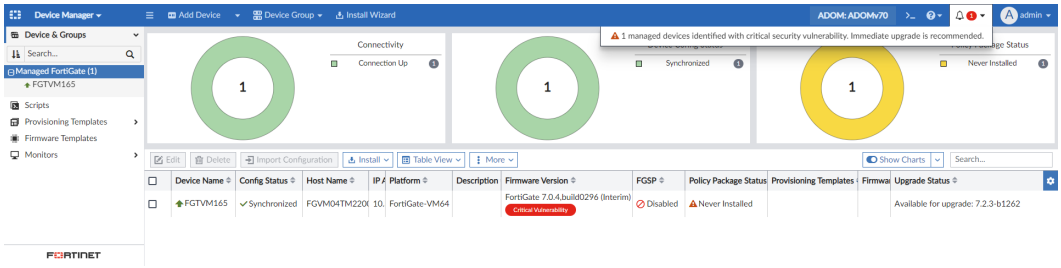

- The following example shows when *Automatically Install Used IPS Profiles to ADOM Devices* is selected, but there are no changes to the IPS header/footer or no installed devices are updated.



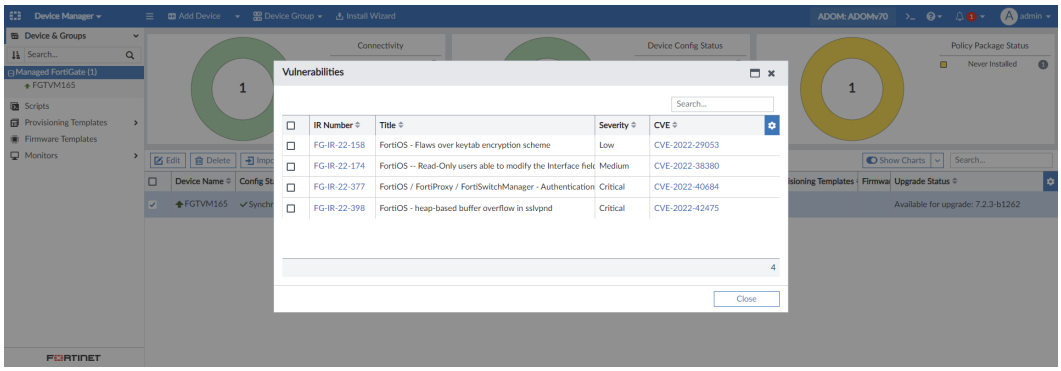

## FortiManager displays PSIRT information when a vulnerability is detected for managed devices - 7.2.2

FortiManager displays PSIRT information and shows a notification when a vulnerability is detected for managed devices.

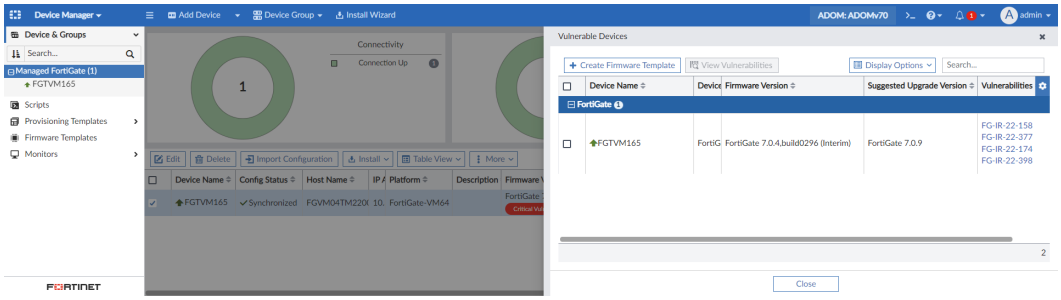
The notification will display in the banner and in the *Firmware Version* column of *Device Manager* > *Device & Groups*. For example, see below:



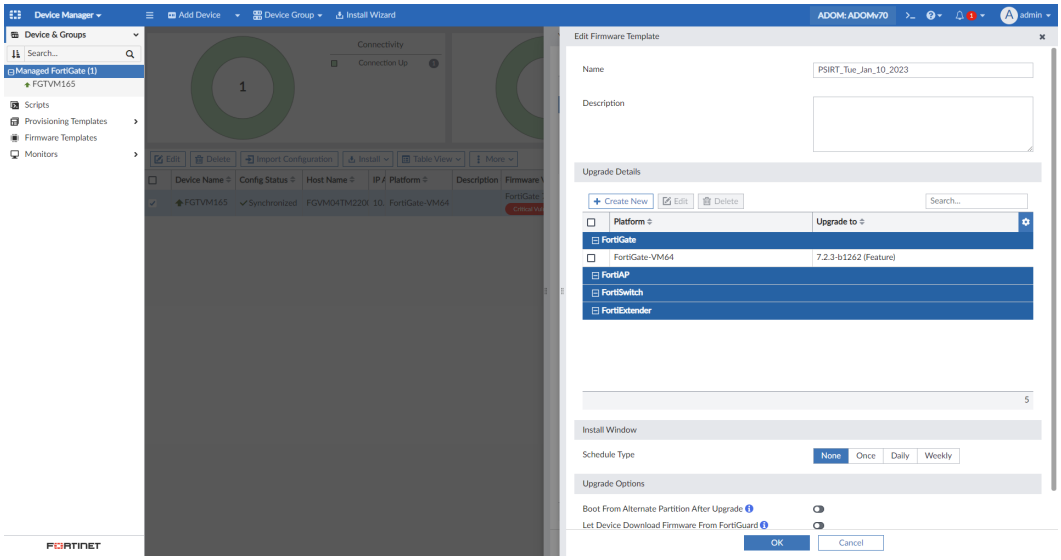

Click the notification in the *Firmware Version* column to display a table view of the PSIRT vulnerabilities for that device. The vulnerabilities are grouped by device type and IR number. You can click the IR number or the CVE to review more information, if needed. For example, clicking `FG-IR-22-158` in the example below would open https://www.fortiguard.com/psirt/FG-IR-22-158.



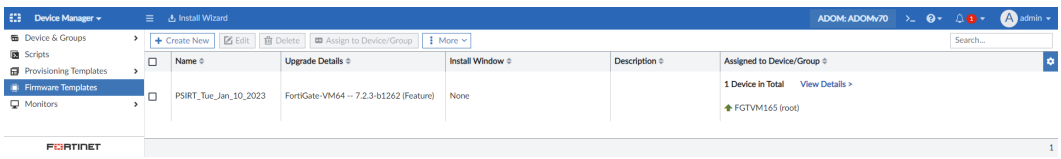

Alternatively, you can click the notification in the banner to open a *Vulnerable Devices* pane with a table of the vulnerable devices. You can click the IR number to review more information, if needed.




In the *Vulnerable Devices* pane, you can click *Create Firmware Template* to upgrade the affected devices. The name of the firmware template is automatically generated.




Once saved, the firmware template can be found in *Device Manager* > *Firmware Templates* and it can be used for the upgrade.

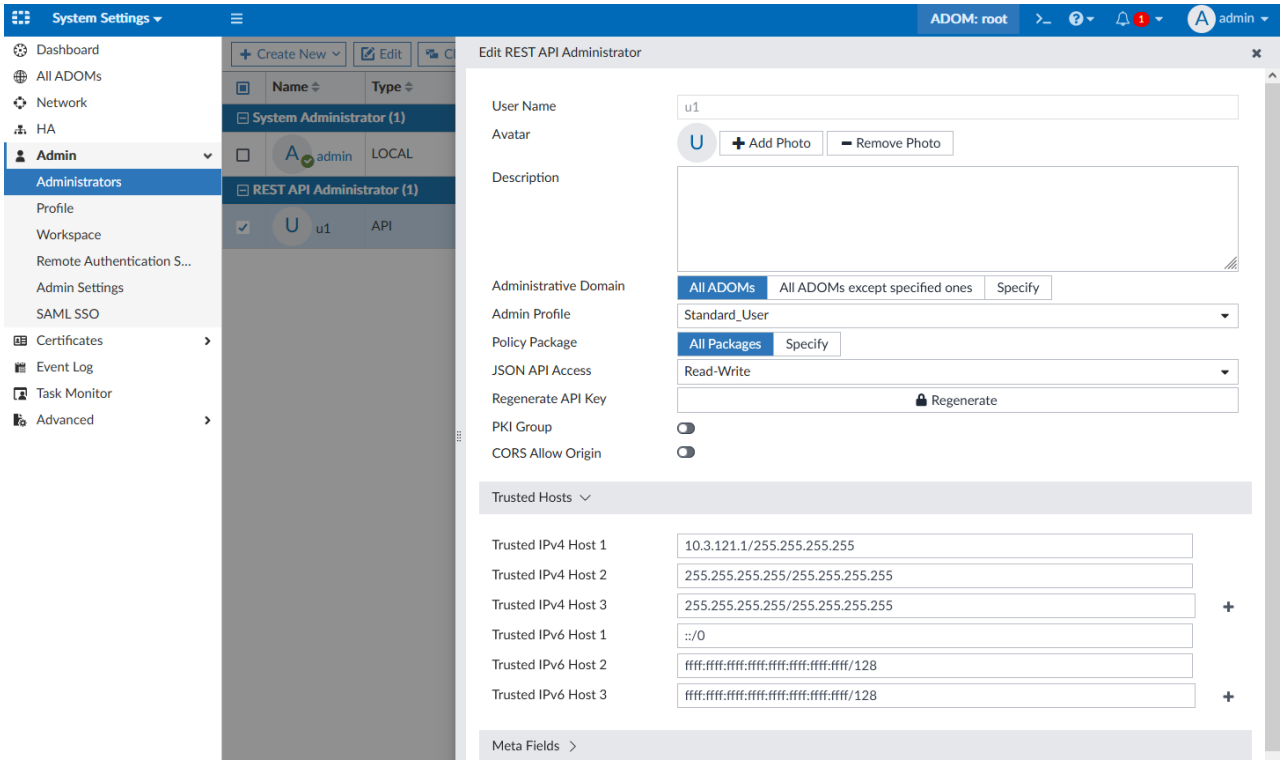


## FortiManager supports authentication token for API administrators - 7.2.2

FortiManager supports authentication token for API administrators.

**To configure REST API administrators with authentication token:**

1. Go to *System Settings* > *Admin* > *Administrators*.
2. Click *Create New* > *REST API Admin*.
   You can configure your REST API administrator using the GUI.




**To configure REST API administrators in the CLI:**

1. Enter the following commands to configure the REST API administrator:

```
config system admin user
   (user)# edit u1
   new entry 'u1' added
      (u1)# set user_type api
      (u1)# set profileid Super_User
           Super user profile selected, adom-access will be set to all
      (u1)# set rpc-permit read-write
      (u1)# set trusthost1 10.3.121.1/16
      (u1)# get
      userid : u1
      login-max : 32
      password : *
      change-password : enable
      trusthost1 : 10.10.121.1 255.255.0.0
      trusthost2 : 255.255.255.255 255.255.255.255
      trusthost3 : 255.255.255.255 255.255.255.255
```

```
        trusthost4 : 255.255.255.255 255.255.255.255
        trusthost5 : 255.255.255.255 255.255.255.255
        trusthost6 : 255.255.255.255 255.255.255.255
        trusthost7 : 255.255.255.255 255.255.255.255
        trusthost8 : 255.255.255.255 255.255.255.255
        trusthost9 : 255.255.255.255 255.255.255.255
        trusthost10 : 255.255.255.255 255.255.255.255
        ipv6_trusthost1 : ::/0
        ipv6_trusthost2 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
        ipv6_trusthost3 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
        ipv6_trusthost4 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
        ipv6_trusthost5 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
        ipv6_trusthost6 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
        ipv6_trusthost7 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
        ipv6_trusthost8 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
        ipv6_trusthost9 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
        ipv6_trusthost10 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
        profileid : Super_User
        dev-group : (null)
        description : (null)
        user_type : api
        ssh-public-key1 :
        ssh-public-key2 :
        ssh-public-key3 :
        avatar : (null)
        meta-data:
        == [ Contact Email ]
        fieldname: Contact Email
        == [ Contact Phone ]
        fieldname: Contact Phone
        fingerprint : (null)
        subject : (null)
        ca : (null)
        cors-allow-origin : (null)
        rpc-permit : read-write
        use-global-theme : enable
        last-name : (null)
        first-name : (null)
        email-address : (null)
        phone-number : (null)
        mobile-number : (null)
        pager-number : (null)
        hidden : 0
        dashboard-tabs:
        dashboard:
    (u1)# end
```

2. Enter the following command to generate a new API key for the administrator.

```
execute api-user generate-key u1
   New API key: 97f3cnrxht4nrkf1mnutb320000000
```

3. Send JSON request to FortiManager with the generated API key in HTTP URL.
   For example:

```
C:\test>curl https://10.10.171.13/jsonrpc?access_token=97f3cnrxht4nrkf1mnutb320000000-
     ksS -d "{\"id\":2,\"method\":\"get\",\"params\":[{\"url\": \"/sys/status\"}]}"
{
   "id": 2,
   "result": [
```

```
        {
        "data": {
           "Admin Domain Configuration": "Enabled",
           "BIOS version": "04000002",
           "Branch Point": "1334",
           "Build": "1334",
           "Current Time": "Thu Feb 02 23:07:16 PST 2023",
           "Daylight Time Saving": "Yes",
           "FIPS Mode": "Disabled",
           "HA Mode": "Stand Alone",
           "Hostname": "FMG-VM64",
           "License Status": "Valid",
           "Major": 7,
           "Max Number of Admin Domains": 1000000000,
           "Max Number of Device Groups": 1000000000,
           "Minor": 2,
           "Offline Mode": "Disabled",
           "Patch": 2,
           "Platform Full Name": "FortiManager-VM64",
           "Platform Type": "FMG-VM64",
           "Release Version Information": " (GA)",
           "Serial Number": "FMG-VM0A11000137",
           "TZ": "US/Pacific",
           "Time Zone": "(GMT-8:00) Pacific Time (US & Canada).",
           "Version": "v7.2.2-build1334 230201 (GA)",
           "x86-64 Applications": "Yes"
        },
        "status": {
           "code": 0,
           "message": "OK"
        },
        "url": "/sys/status"
        }
     ]
  }
```


4. Send JSON request to FortiManager with the generated API key in HTTP header.
   For example:

```
C:\test>curl https://10.10.171.13/jsonrpc -H "Authorization:Bearer
     97f3cnrxht4nrkf1mnutb320000000" -ksS -d "
     {\"id\":2,\"method\":\"get\",\"params\":[{\"url\": \"/sys/status\"}]}"
{
   "id": 2,
   "result": [
      {
         "data": {
         "Admin Domain Configuration": "Enabled",
         "BIOS version": "04000002",
         "Branch Point": "1334",
         "Build": "1334",
         "Current Time": "Thu Feb 02 23:11:34 PST 2023",
         "Daylight Time Saving": "Yes",
         "FIPS Mode": "Disabled",
         "HA Mode": "Stand Alone",
         "Hostname": "FMG-VM64",
         "License Status": "Valid",
         "Major": 7,
         "Max Number of Admin Domains": 1000000000,
```

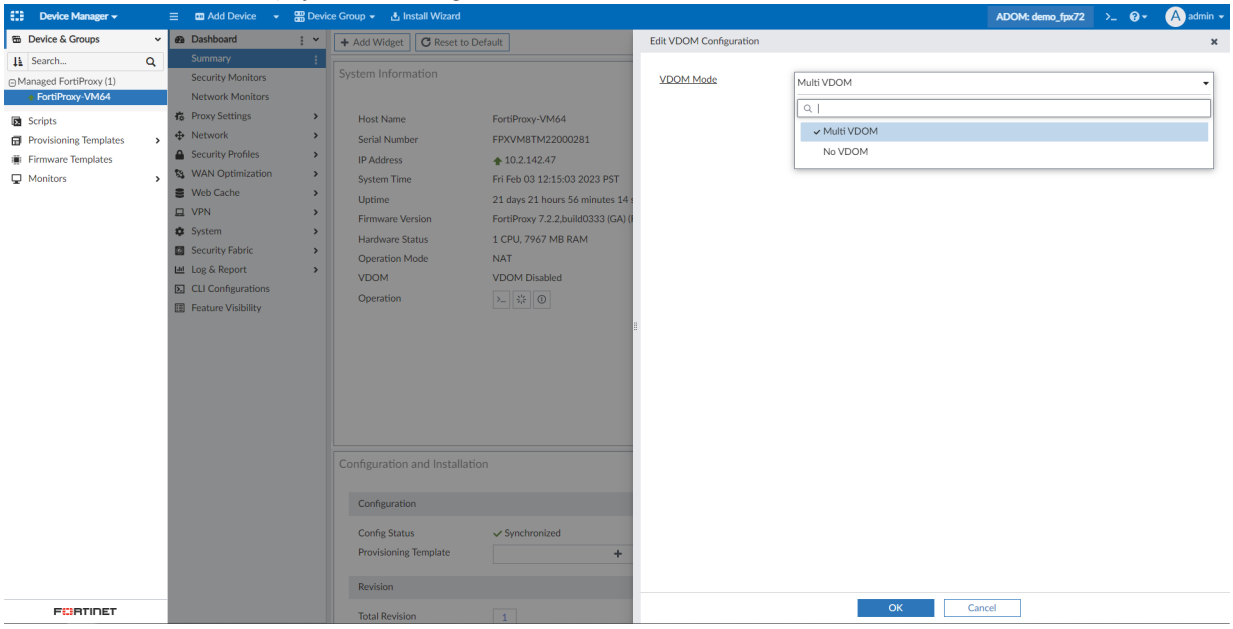
```
            "Max Number of Device Groups": 1000000000,
            "Minor": 2,
            "Offline Mode": "Disabled",
            "Patch": 2,
            "Platform Full Name": "FortiManager-VM64",
            "Platform Type": "FMG-VM64",
            "Release Version Information": " (GA)",
            "Serial Number": "FMG-VM0A11000137",
            "TZ": "US/Pacific",
            "Time Zone": "(GMT-8:00) Pacific Time (US & Canada).",
            "Version": "v7.2.2-build1334 230201 (GA)",
            "x86-64 Applications": "Yes"
         },
         "status": {
            "code": 0,
            "message": "OK"
         },
         "url": "/sys/status"
         }
      ]
   }
```


## FortiProxy 7.2 ADOM type added support for VDOMs - 7.2.2

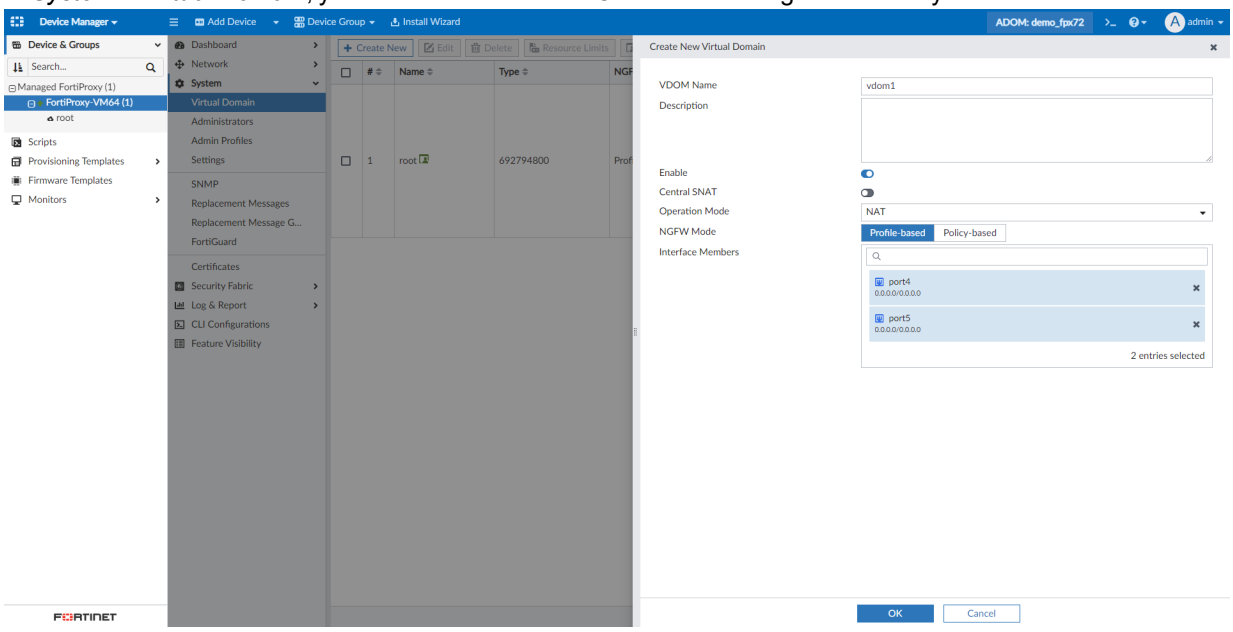
FortiProxy 7.2 ADOM type added support for VDOMs.

**To manage VDOMs in a FortiProxy 7.2 ADOM:**

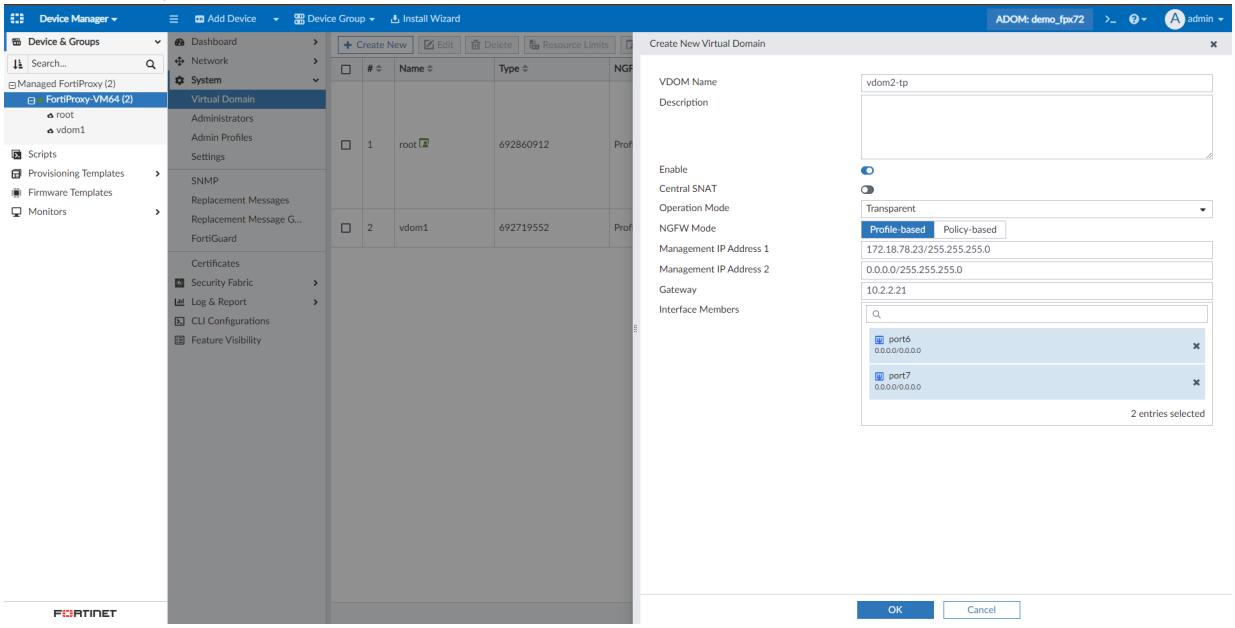
1. Go to *Device Manager* and select a managed FortiProxy device to enter the Device Database.
2. In *Dashboard* > *Summary*, you can change the VDOM mode for the selected device.



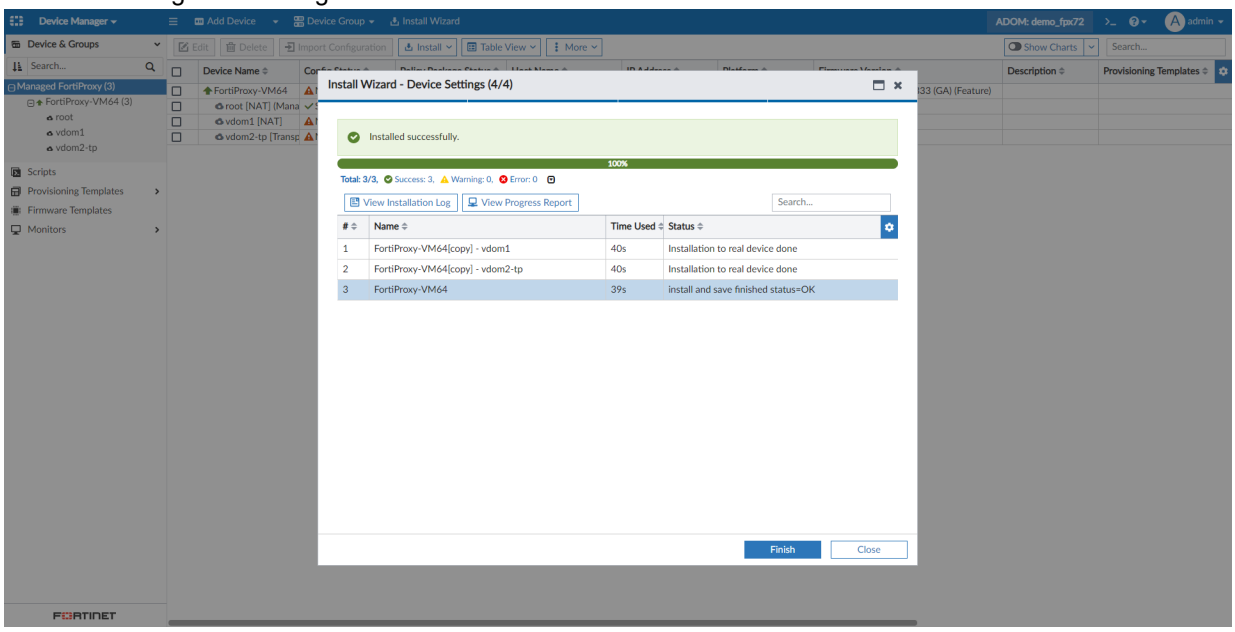
3. In *System* > *Virtual Domain*, you can create a new VDOM for the managed FortiProxy device.




4. Create a transparent VDOM.



5. Install the changes to the target device.



# Policy and Objects

This section lists the new features added to FortiManager for policy and objects:



## Policy

This section lists the new features added to FortiManager for policies:



### Policy Packages can use colors for sections

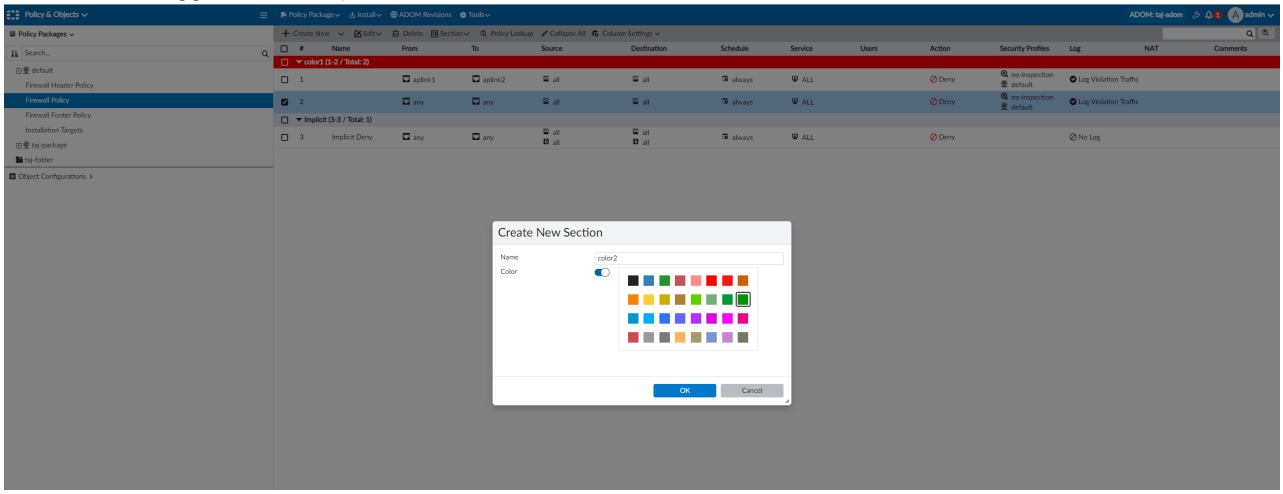
Policy Packages can use colors for sections to help the administrators easily differentiate between policies.

For example, as an administrator you could include a red section for external traffic, blue section for internal traffic, and orange section as production.

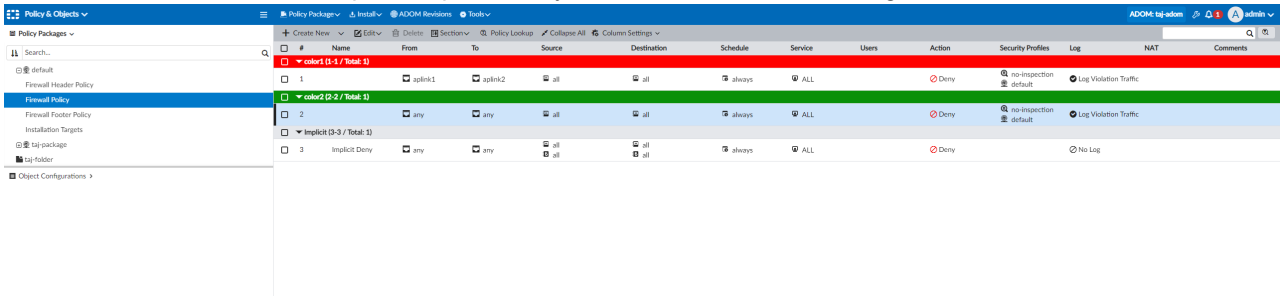
**To create a policy section with color:**

1. Go to *Policy & Objects* > *Policies*, and select a policy package.
2. Highlight a policy, and click *Section* > *Add* from the toolbar.
3. Enter a name for the section.

4. Set the Color toggle to the ON position, and then select a color.

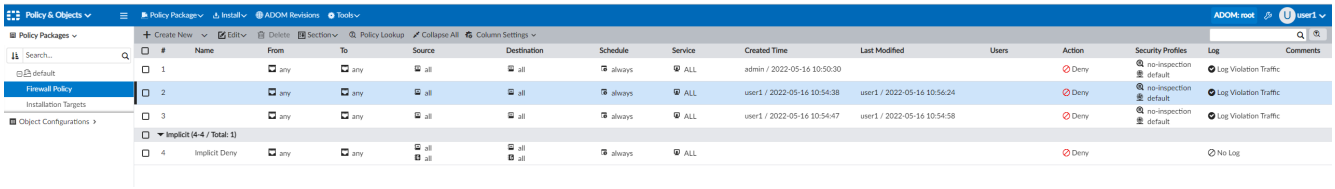



5. Click *OK*.
The section title is added to the policies pane with your chosen color as the background.



## Firewall policy creator exposed - 7.2.1

The *Created Time* and *Last Modified* fields display the name of the admin who created or last modified the policy along with the creation or modification timestamp.

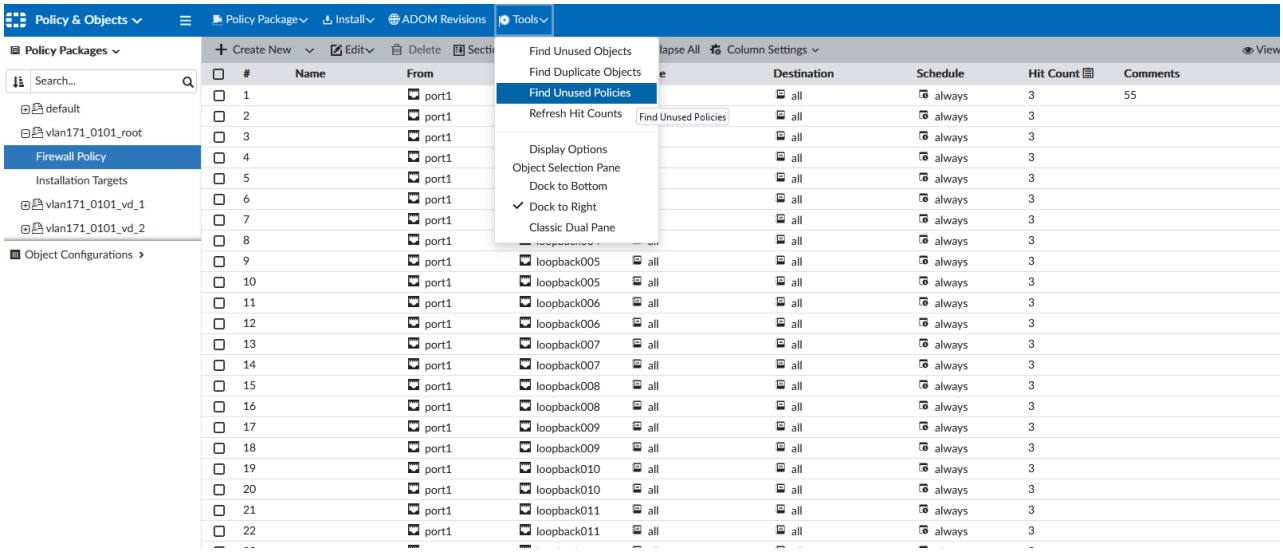


## Unused Policies filter in a predefined time frame to help security teams for audit purposes

You may filter the unused policies report by date range to find policies that have not been used within that particular date range.

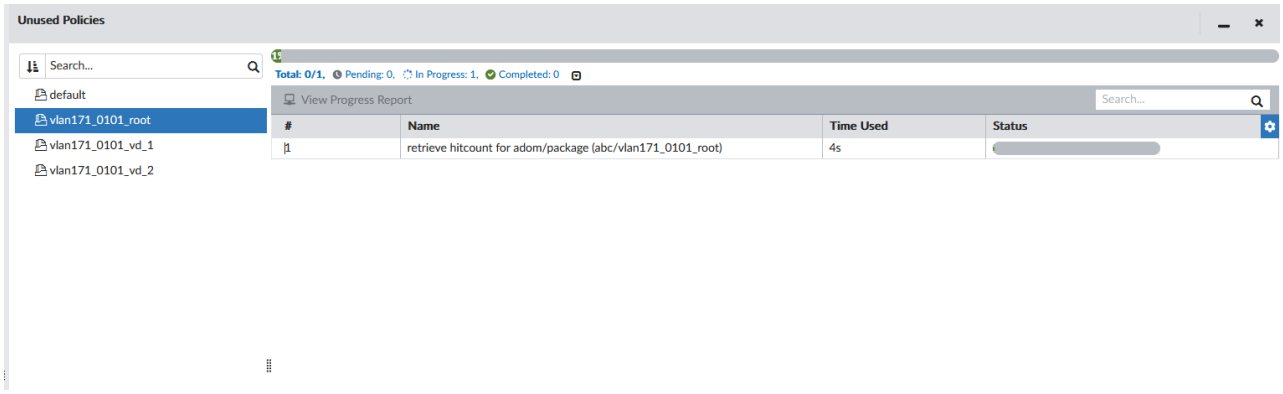
**To filter the report:**

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. From the *Tools* dropdown menu in the toolbar, select *Find Unused Policies*.

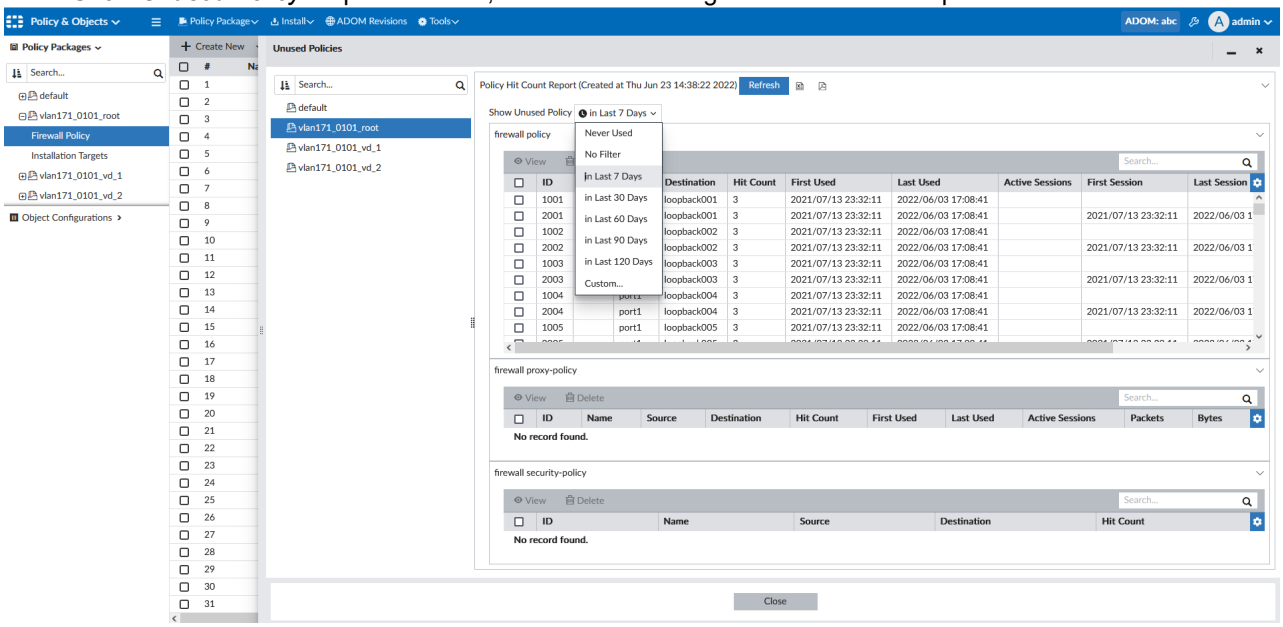



The *Unused Policies* window opens.

4. If needed, click the *Refresh* button to retrieve the hitcount data from the FortiGate. Wait for the process to finish.



5. In the *Show Unused Policy* dropdown menu, select the date range within which the report should be filtered.



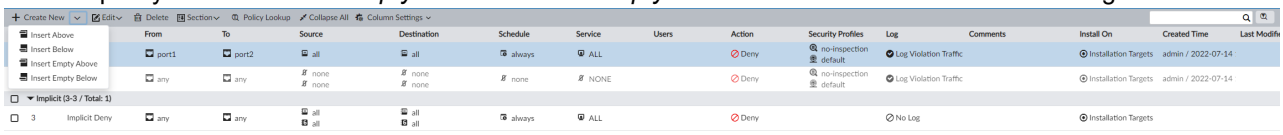

Any policies that have not been used within this date range are displayed. For example, to find policies that have not been used in the last 7 days, select "in Last 7 Days" from the dropdown menu.

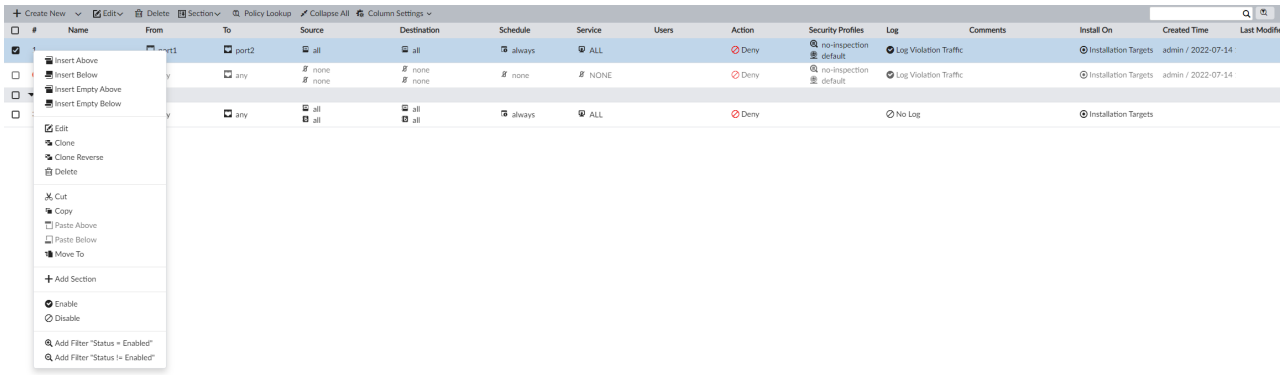
## The Insert Empty Policy operation will insert a new disabled policy above or below, with no interface pair inheritance from the adjacent policies - 7.2.1

Insert a new empty firewall policy above or below the currently selected policy. These options are available from the policy *Create New* dropdown menu and the policy right-click menu.

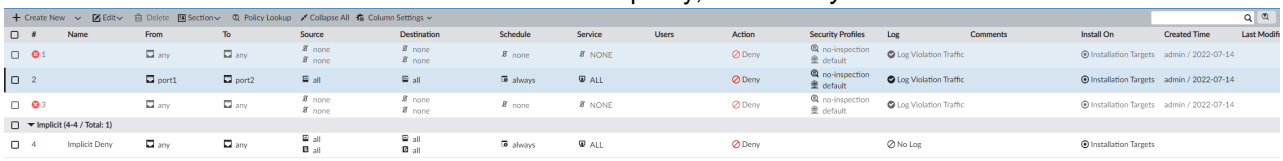
**To insert a new empty policy:**

1. Go to *Policy & Objects* > *Policy Packages* > *Firewall Policy*.
2. Select a policy and click *Insert Empty Above* or *Insert Empty Below* in the *Create New* menu or the right-click menu.





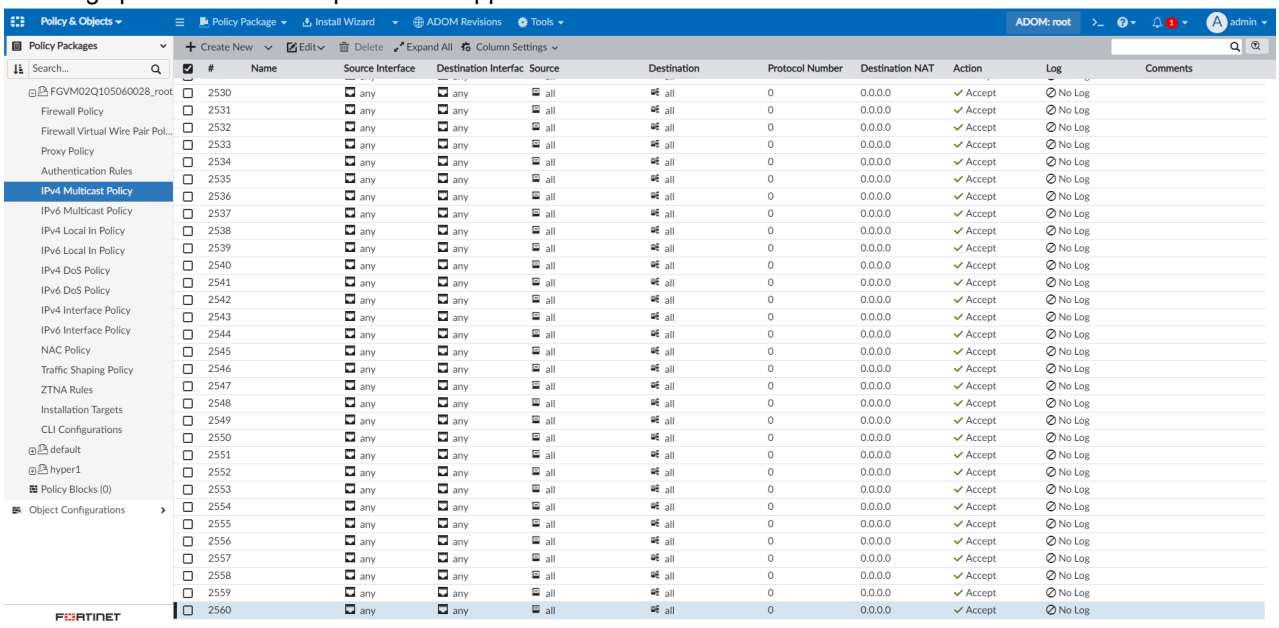
The new empty policy is inserted above or below the selected policy as a default deny policy. Source and destination interfaces are not inherited from the selected policy, and use *any*.



## Increased number of multicast policies to 2560 per policy package - 7.2.2

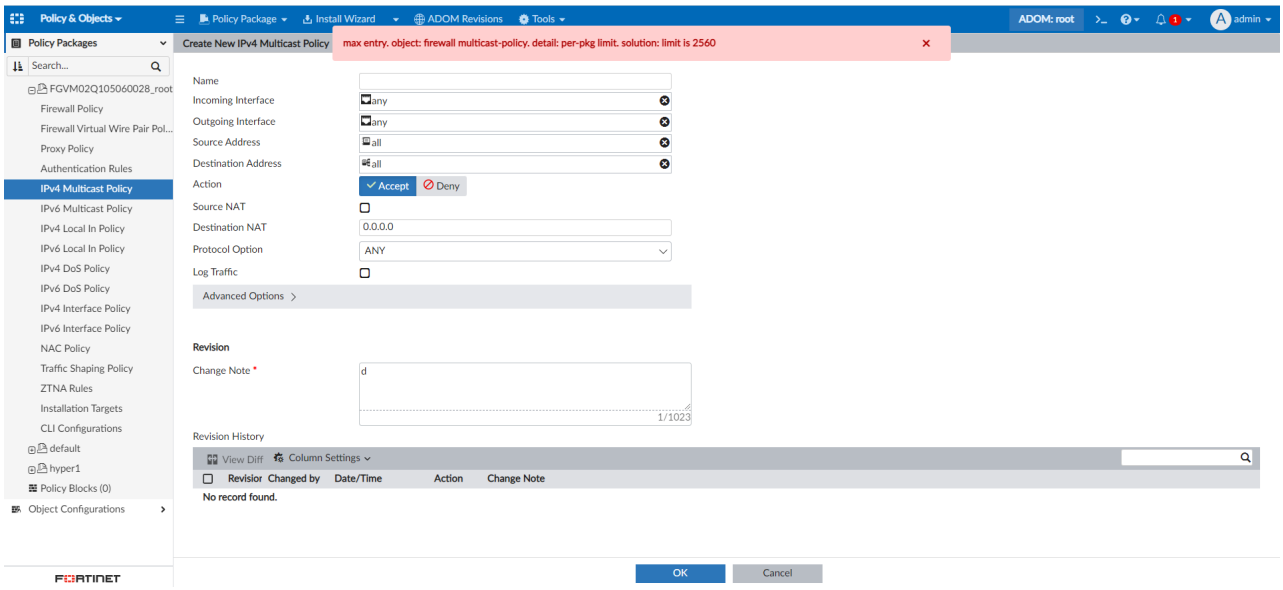
The number of allowed multicast policies has been in creased to 2560 per policy package.

- Creating up to 2560 multicast policies is supported.



- When creating the 2561st policy, the GUI gives the following error: max entry. object: `firewall multicast-`

```
policy. detail: per-pkg limit. solution: limit is 2560.
```

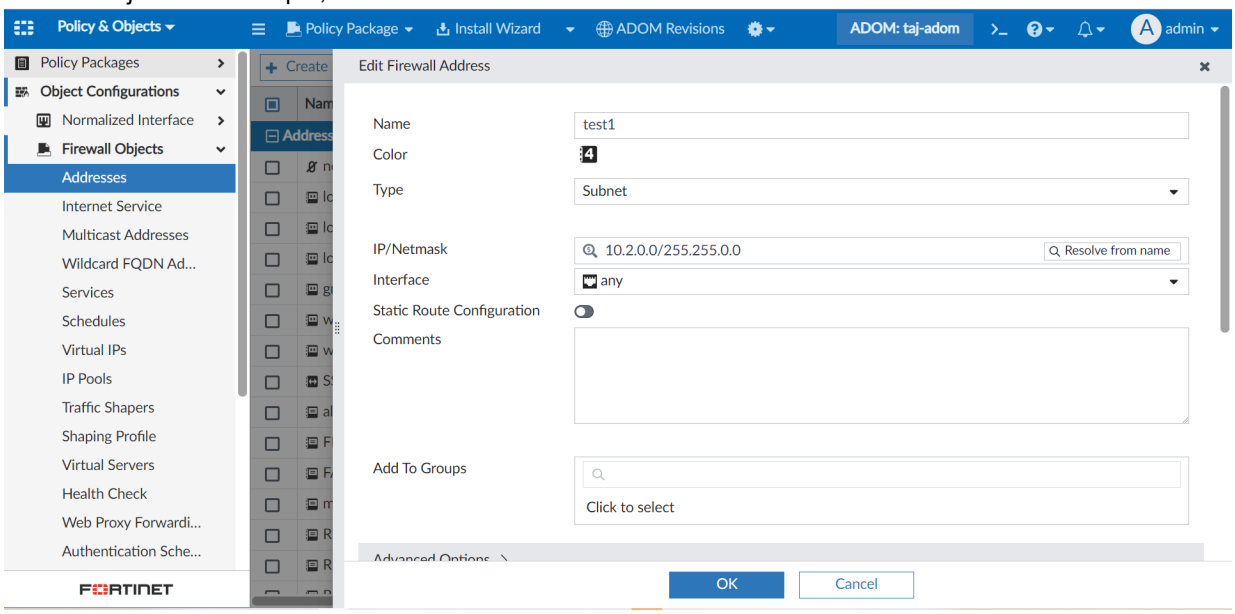



## Firewall policy strict search option will return only the results with an exact match - 7.2.2

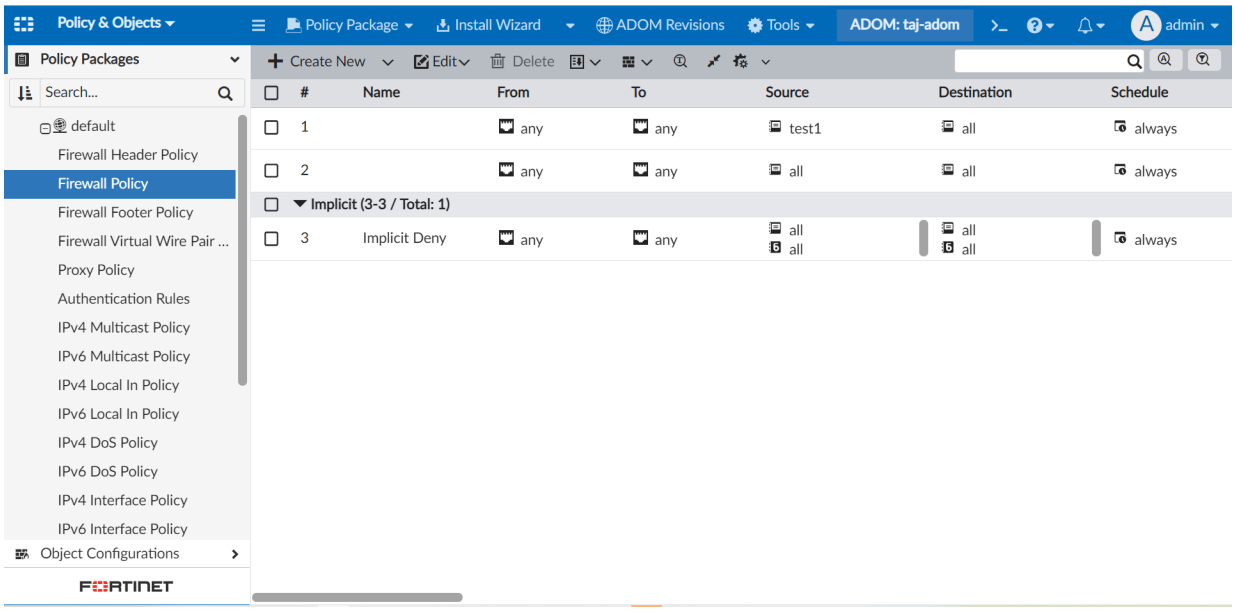
Firewall policy strict search option will return only the results with an exact match.

**To use strict search in a Firewall policy:**

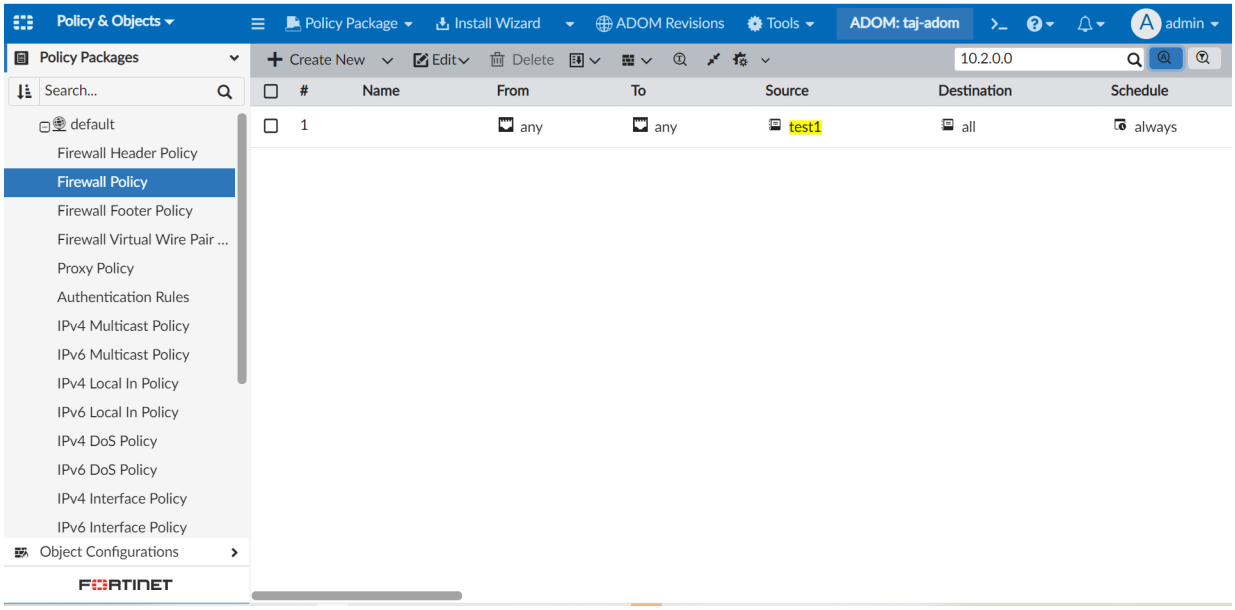
1. Go to *Policy & Objects* > *Firewall Policy*. The strict search icon is displayed next to the search bar. When enabled, search results only display exact matches.
2. For example, go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Addresses*, and create a firewall address object. For example, `test1` with the IP `10.2.0.0`.



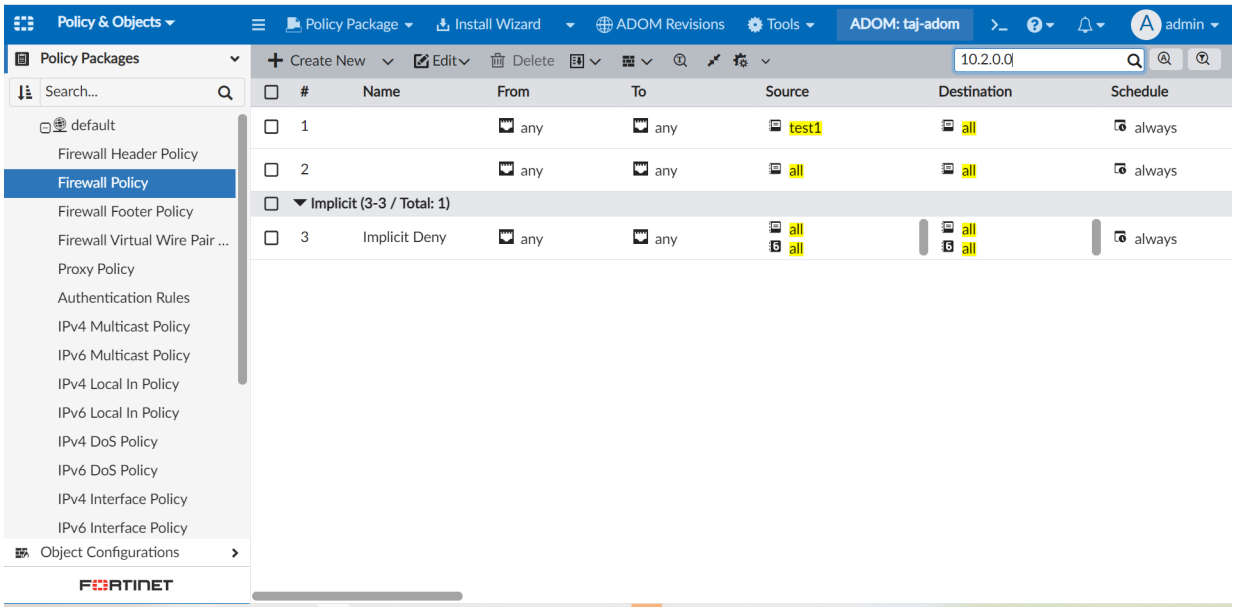
3. Use the firewall address object in a policy, and create a default policy as a comparison.




4. Search for the address *10.2.0.0*. When strict search is enabled, the search result returns only values where there is a total match.

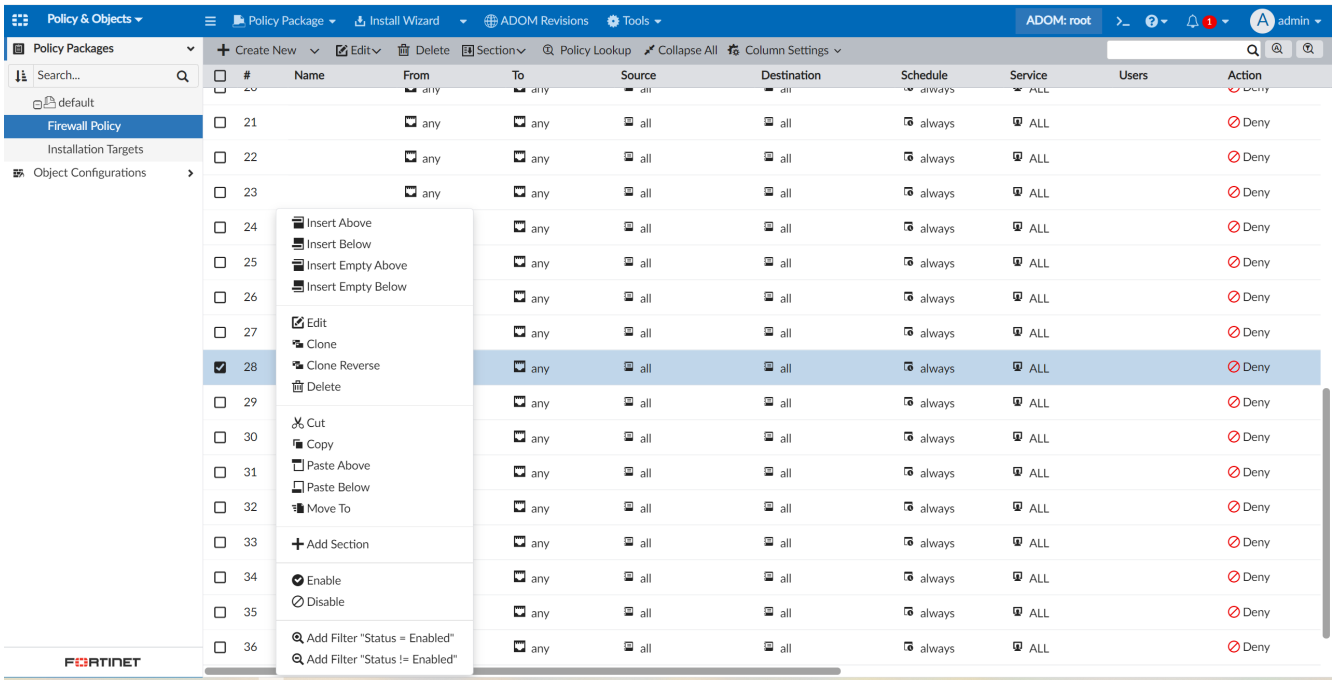


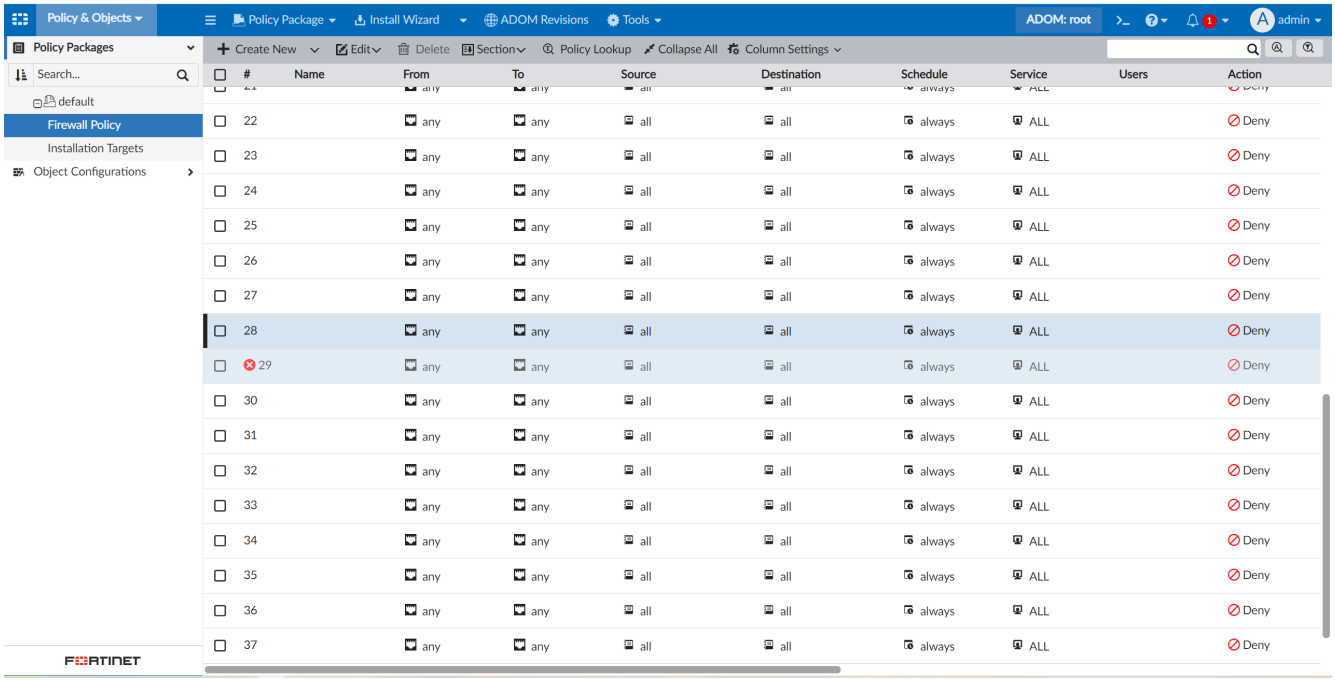
5. When strict search is not enabled, the search also returns "all" as a result.




## Inserting a new policy in the Policy Package page will keep the screen focus and position on the newly added policy - 7.2.2

When a new policy is inserted using one of the right-click *Insert New* options, the policy table remains in the same position rather than scrolling to the new policy.



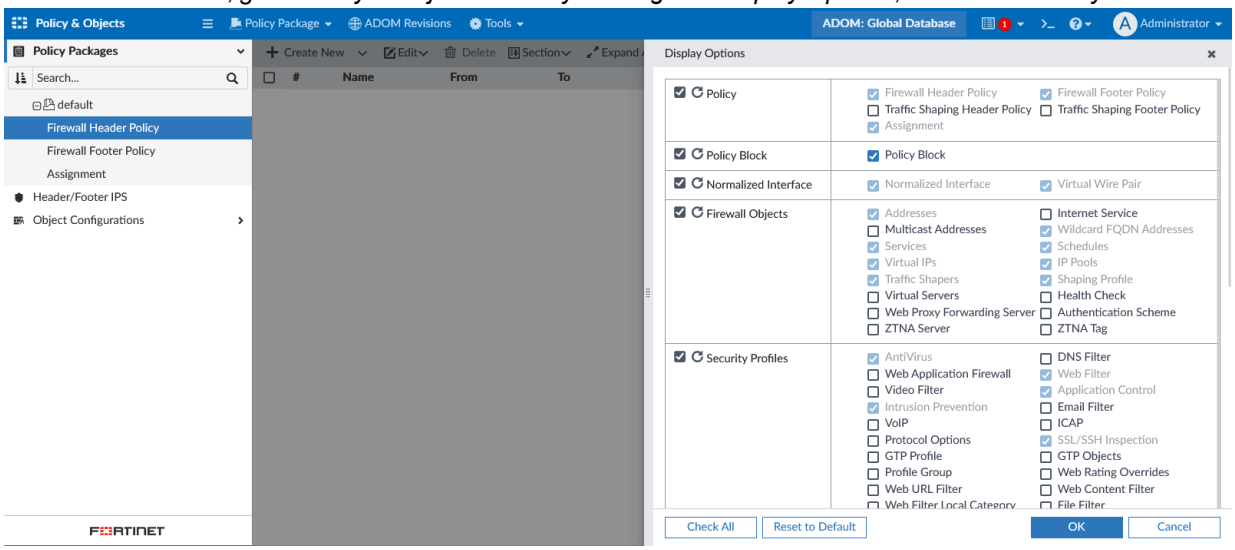



## Policy Blocks are supported in the Global ADOM and can be reused in different Global Policy Packages - 7.2.2

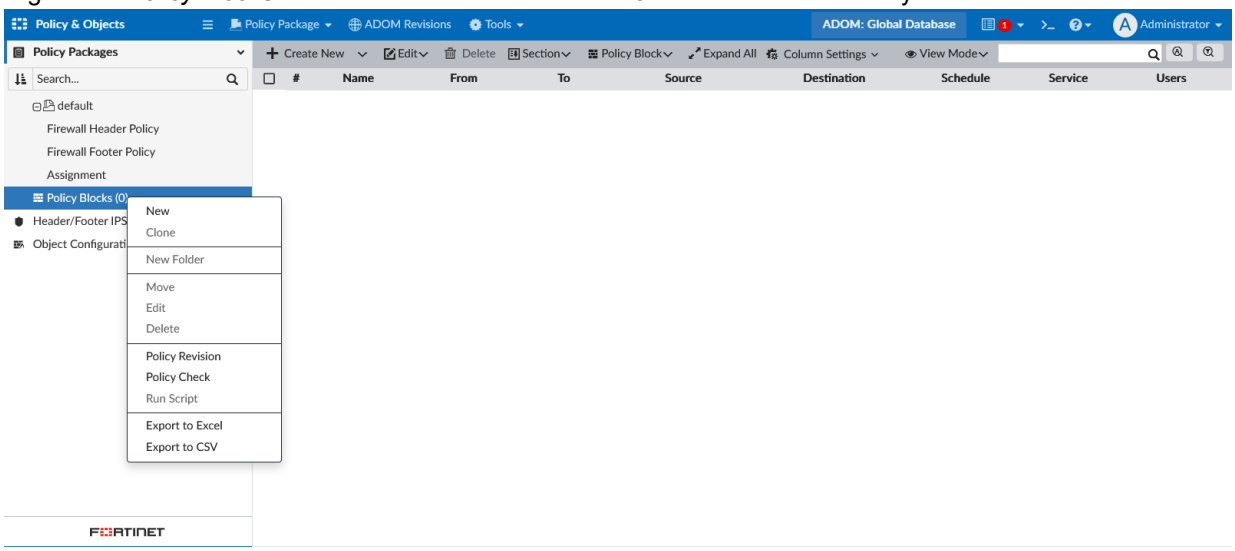
Policy Blocks are supported in the Global ADOM and can be reused in different Global Policy Packages.

**To use policy blocks in Global ADOMs:**

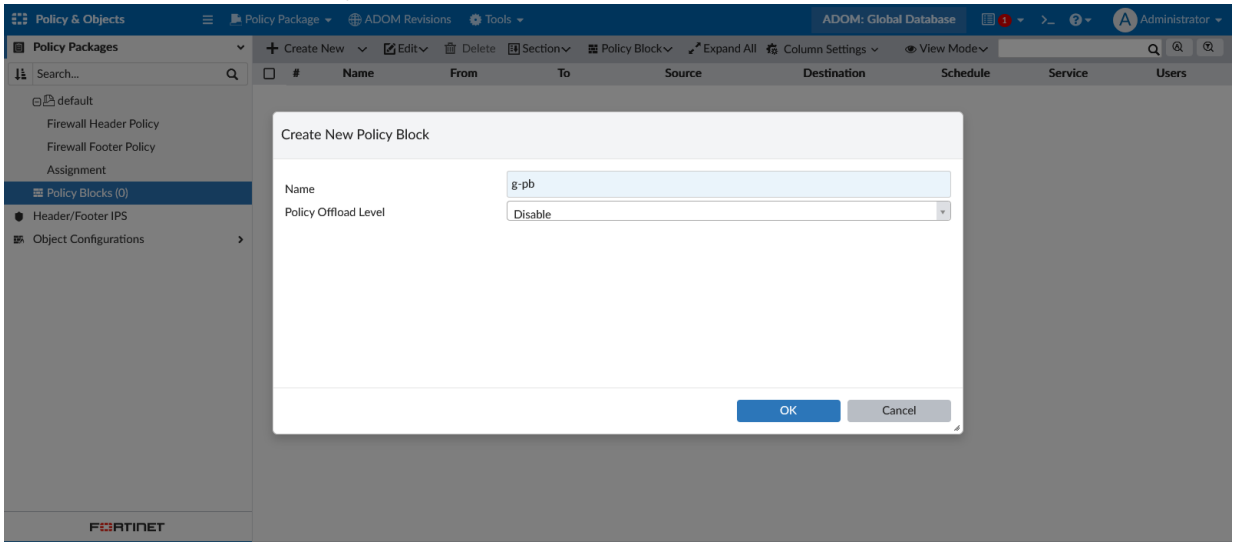
1. In the Global ADOM, go to *Policy & Objects* > *Policy Packages* > *Display Options*, and enable *Policy Block*.



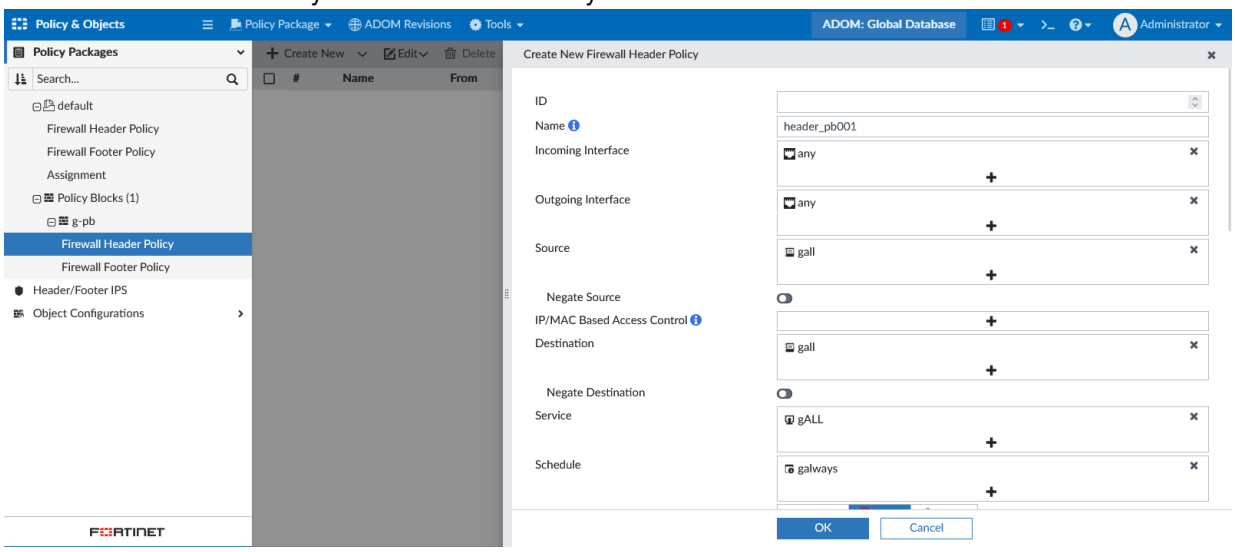
2. Right-click *Policy Blocks* from the tree menu and select *New* to create a new Policy Block.



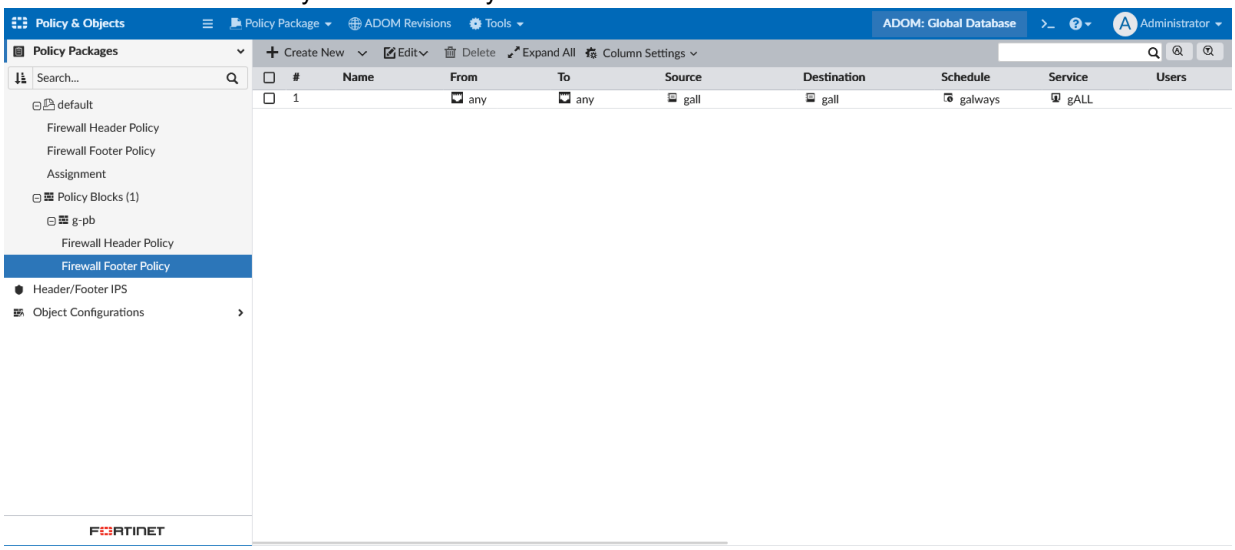

3. Enter a *Name* and set the *Policy Offload Level*, and click *OK*.



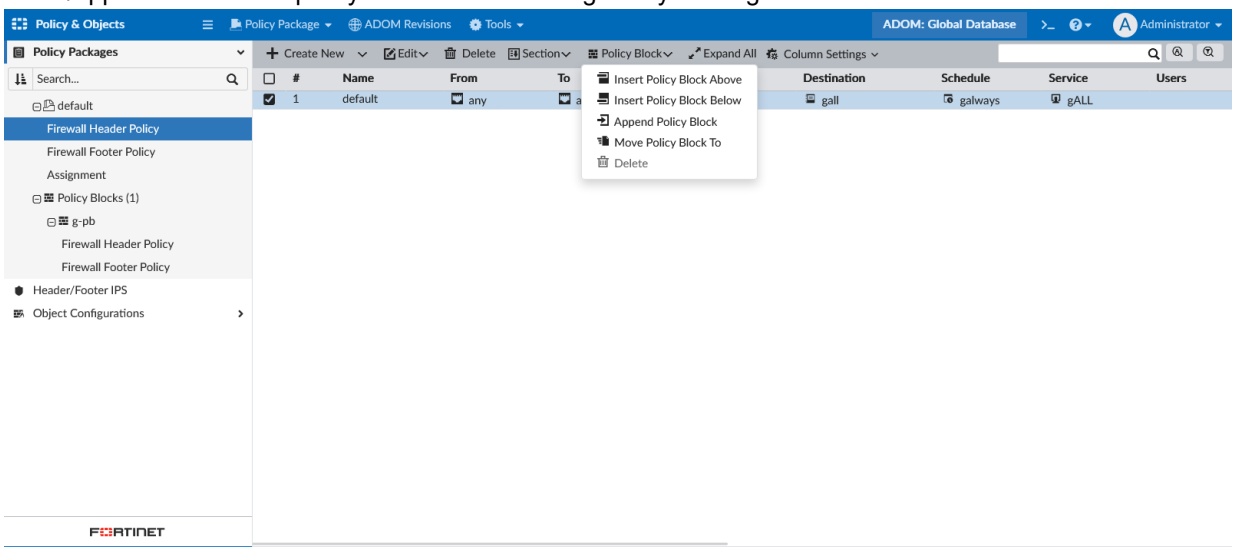
4. Add a Firewall Header Policy under the created Policy Block.



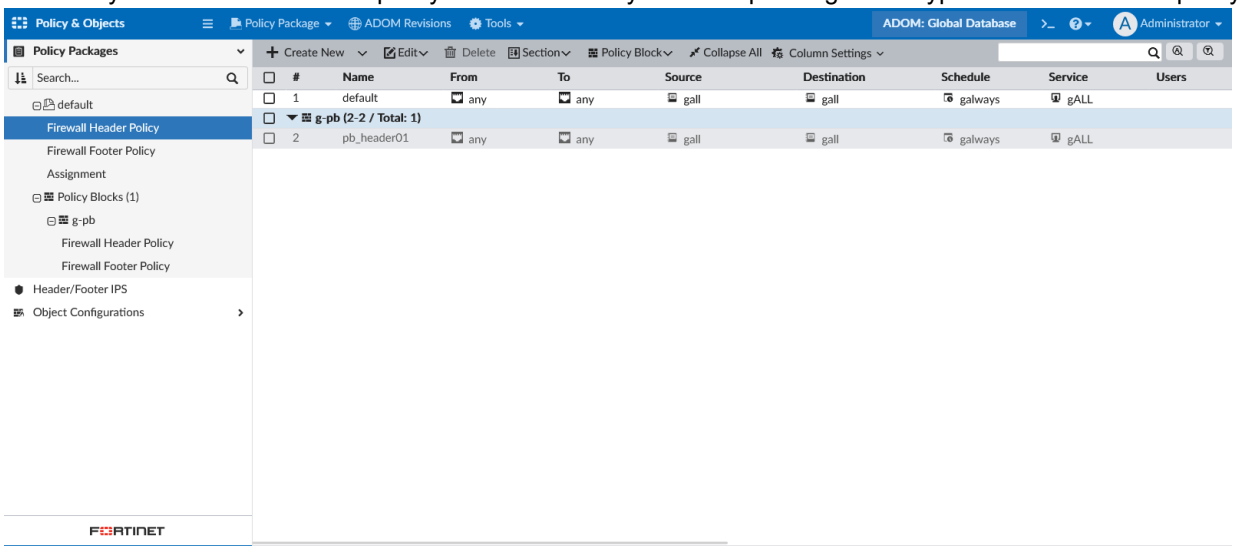

5. Add a Firewall Footer Policy under the Policy Block.



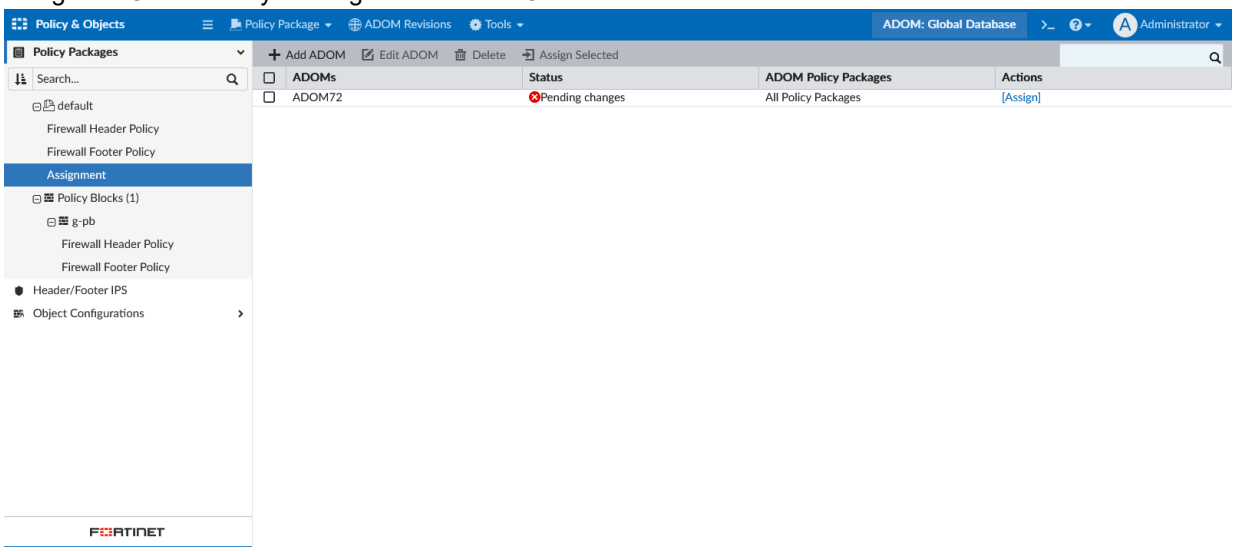
6. Insert/append the created policy block into an existing Policy Package.



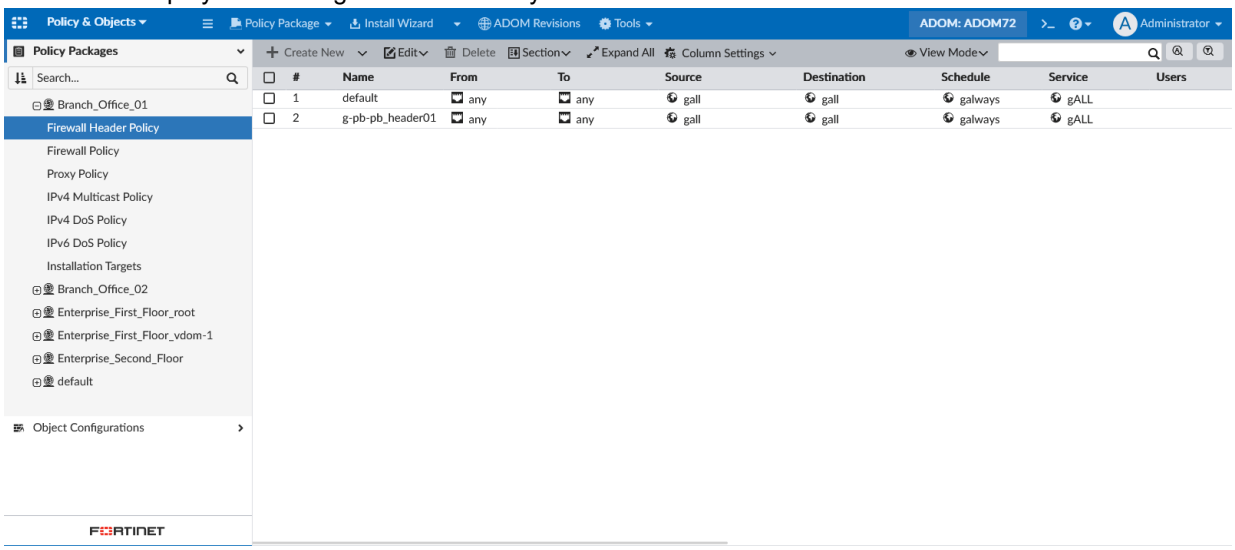

7. The Policy Block header or footer policy will be selectively added depending on the type of current Firewall policy.



8. Assign the Global Policy Package to a local ADOM.



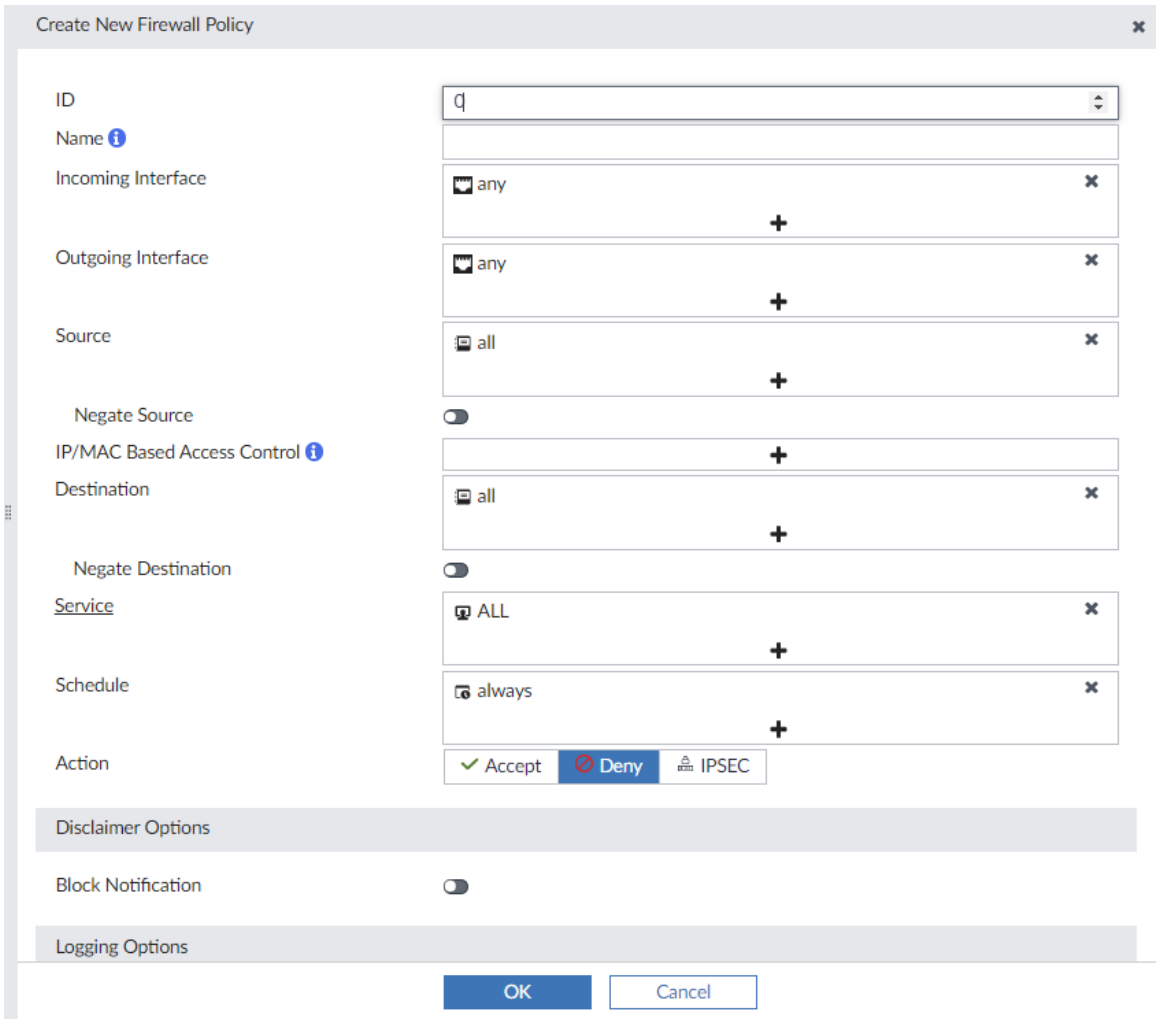

The ADOM displayed the assigned Global Policy Block.

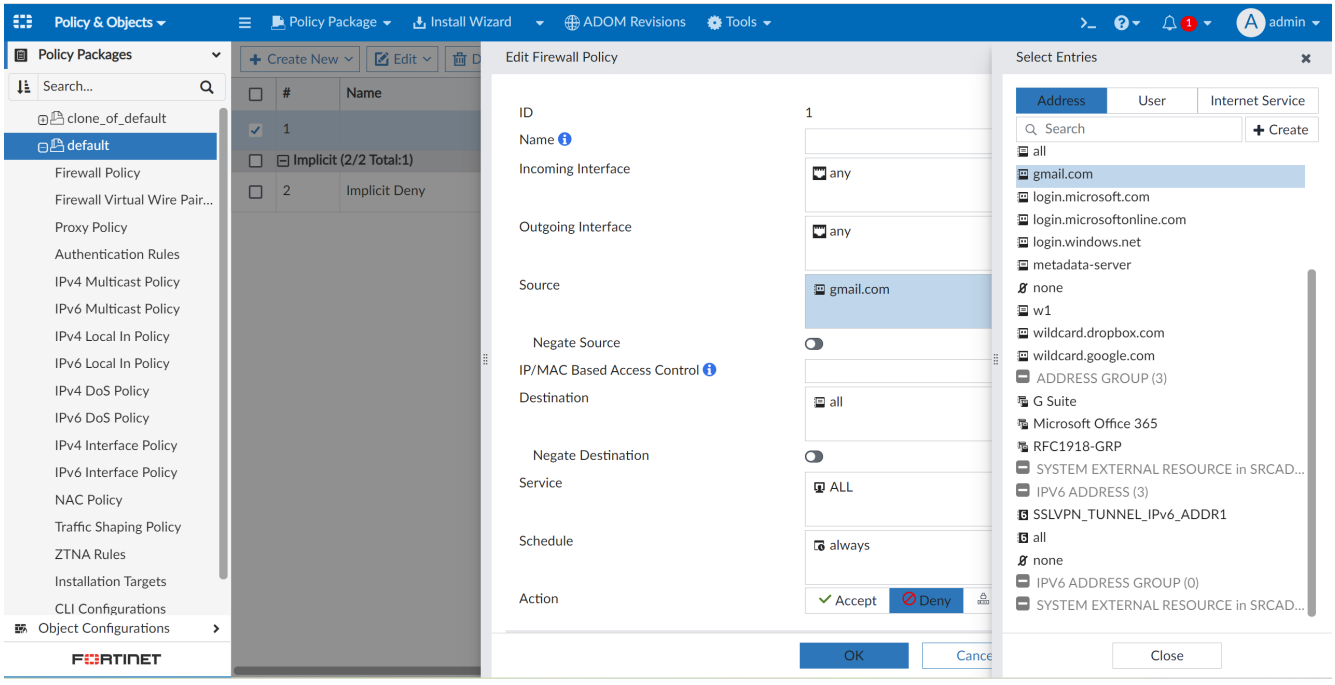


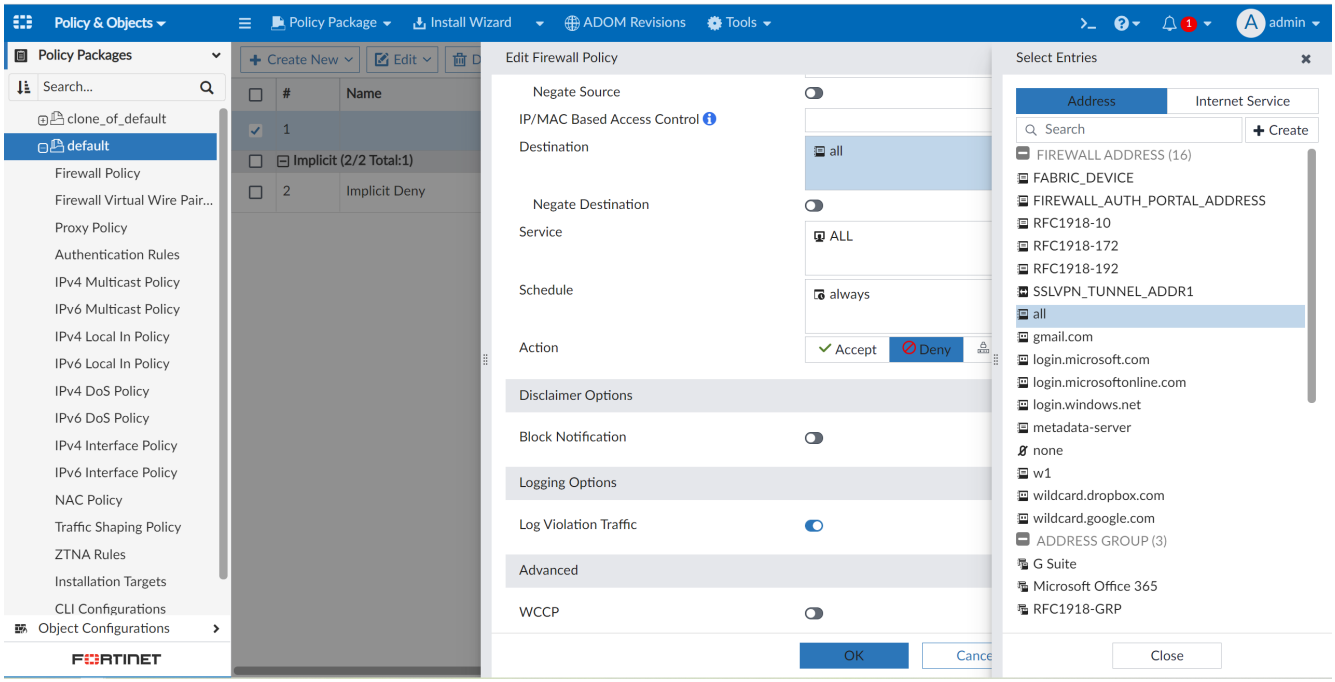

## Create new firewall policy page consolidates source and destination object types - 7.2.2

In the firewall policy forms, source object selection fields (such as IPv4 and IPv6 addresses, users, groups, and FSSO groups) have been consolidated into one *Source* field, similar to FortiGate policy creation forms.

Destination object type fields have been consolidated into one *Destination* field.


Create New Firewall Policy
ID
Name
Incoming Interface
any
Outgoing Interface
any
Source
all
Negate Source
IP/MAC Based Access Control
Destination
all
Negate Destination
Service
ALL
Schedule
always
Action
Accept
Deny
IPSEC
Disclaimer Options
Block Notification
Logging Options
OK
Cancel


Policy & Objects
Policy Package
Install Wizard
ADOM Revisions
Tools
admin
Policy Packages
Search...
clone_of_default
default
Firewall Policy
Firewall Virtual Wire Pair...
Proxy Policy
Authentication Rules
IPv4 Multicast Policy
IPv6 Multicast Policy
IPv4 Local In Policy
IPv6 Local In Policy
IPv4 DoS Policy
IPv6 DoS Policy
IPv4 Interface Policy
IPv6 Interface Policy
NAC Policy
Traffic Shaping Policy
ZTNA Rules
Installation Targets
CLI Configurations
Object Configurations
Create New
Edit
Name
Implicit (2/2 Total:1)
Implicit Deny
Edit Firewall Policy
ID
Name
Incoming Interface
any
Outgoing Interface
any
Source
gmail.com
Negate Source
IP/MAC Based Access Control
Destination
all
Negate Destination
Service
ALL
Schedule
always
Action
Accept
Deny
OK
Select Entries
Address
User
Internet Service
Search
Create
all
gmail.com
login.microsoft.com
login.microsoftonline.com
login.windows.net
metadata-server
none
w1
wildcard.dropbox.com
wildcard.google.com
ADDRESS GROUP (3)
G Suite
Microsoft Office 365
RFC1918-GRP
SYSTEM EXTERNAL RESOURCE in SRCAD...
IPV6 ADDRESS (3)
SSLVPN_TUNNEL_IPv6_ADDR1
all
none
IPV6 ADDRESS GROUP (0)
SYSTEM EXTERNAL RESOURCE in SRCAD...
Close

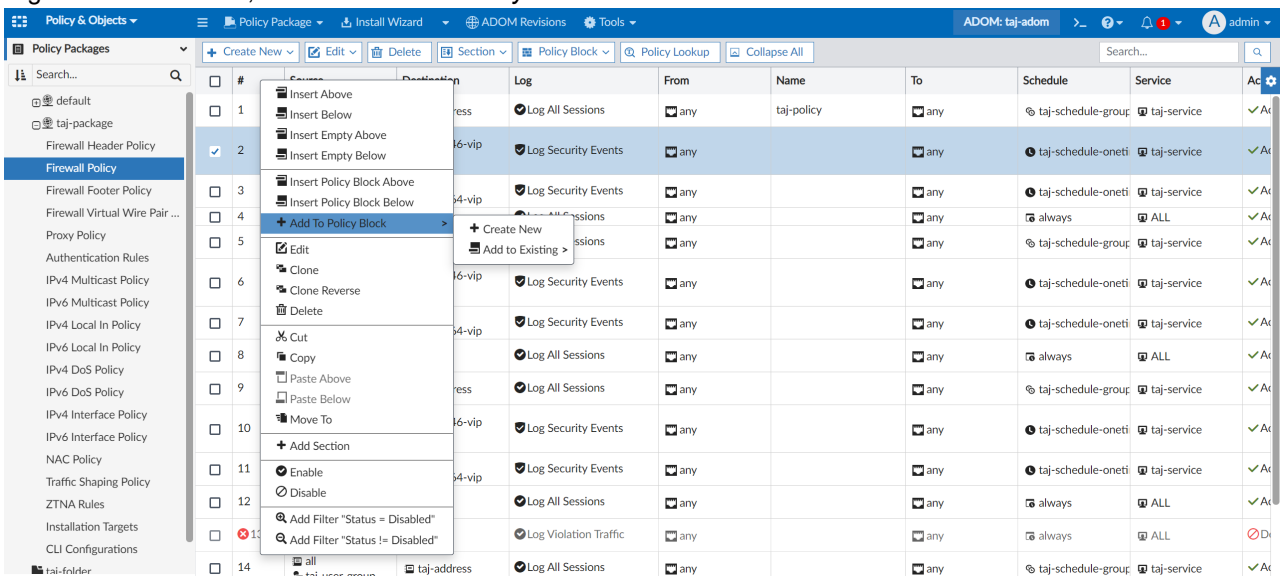



## Create a Policy Block from a selection of the policies within Policy Package - 7.2.2

Create a Policy Block from a selection of the policies within Policy Package.

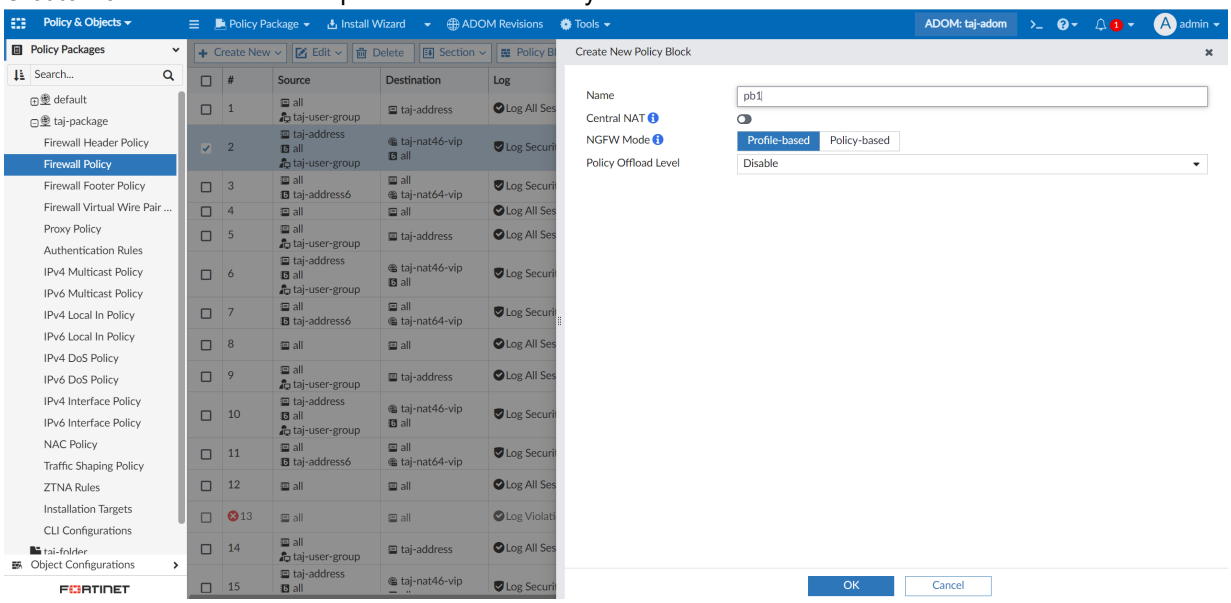
**To add a selection of policies to a Policy Block:**

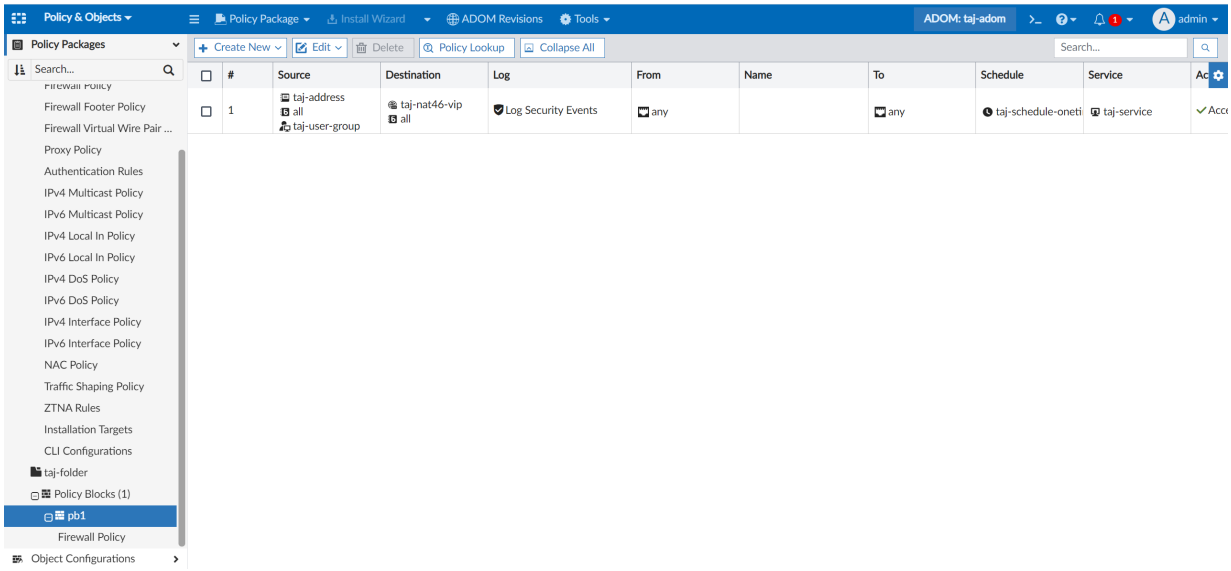
1. Go to *Policy & Objects*, and ensure that Policy Blocks are enabled in *Tools* > *Feature Visibility*.
2. Go to a Policy Package and select multiple policies.
3. Right-click in the table, and select *Add to Policy Block* from the context menu.



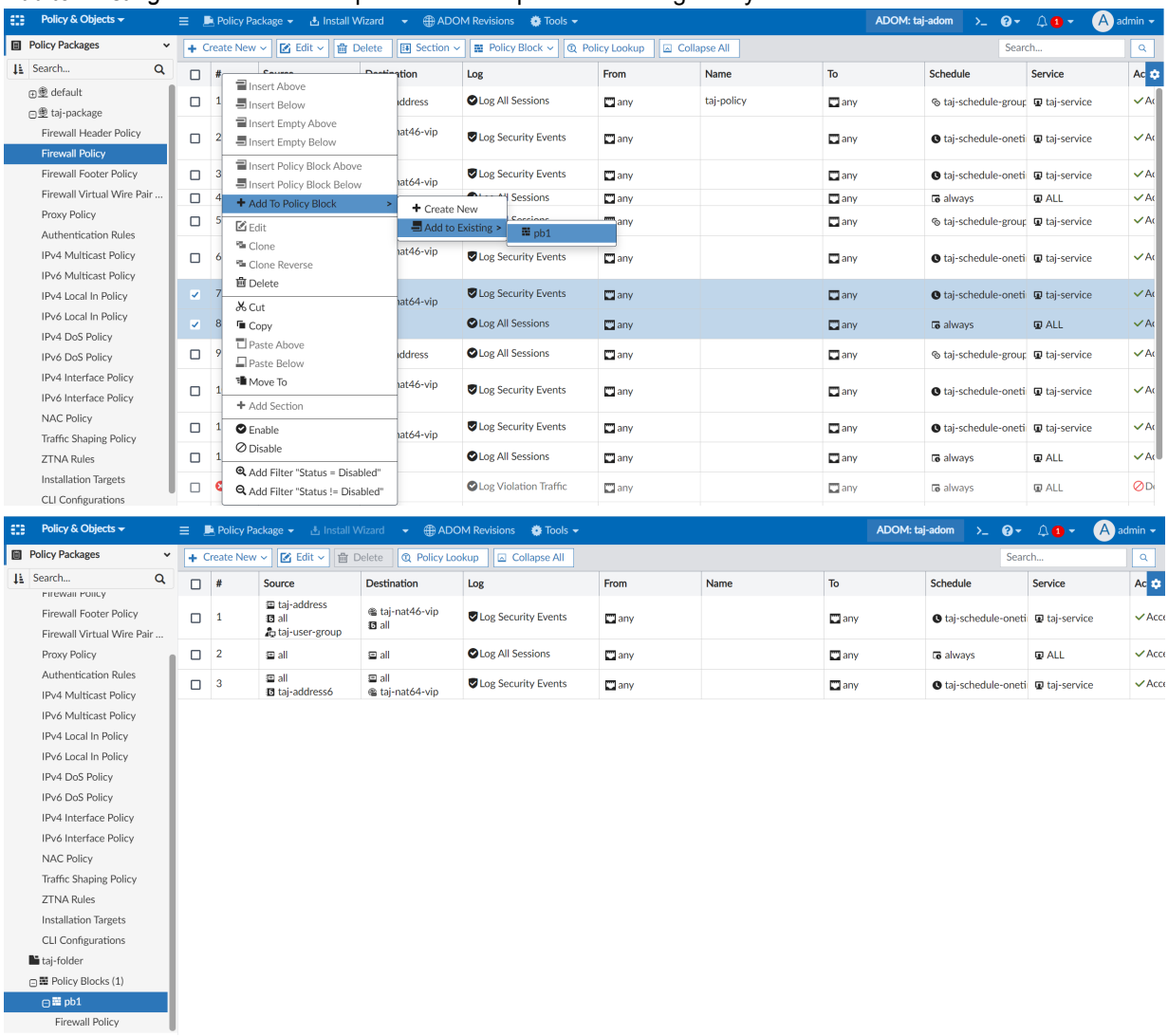

There are two options:

**a.** *Create New*: Add the selected policies to a new Policy Block.



**b.** *Add to Existing*: Add the selected policies to the specified existing Policy Block.




# Objects

This section lists the new features added to FortiManager for objects:

- Resolve IP address from FQDN for firewall address type subnet on page 177
- FortiManager supports empty Address Group on page 180
- Metadata Variables are supported in Firewall Objects configuration on page 182
- Additional filters available for IPS sensors on page 184
- Monitoring page for the IPS on-hold signatures on page 186
- Enhanced object "where used" function 7.2.1 on page 188
- Factory default firewall addresses and address group for private IP space (RFC1918) 7.2.2 on page 190
- Virtual IP (VIP) objects defined as an IP range are now searchable by an IP in the range 7.2.2 on page 191

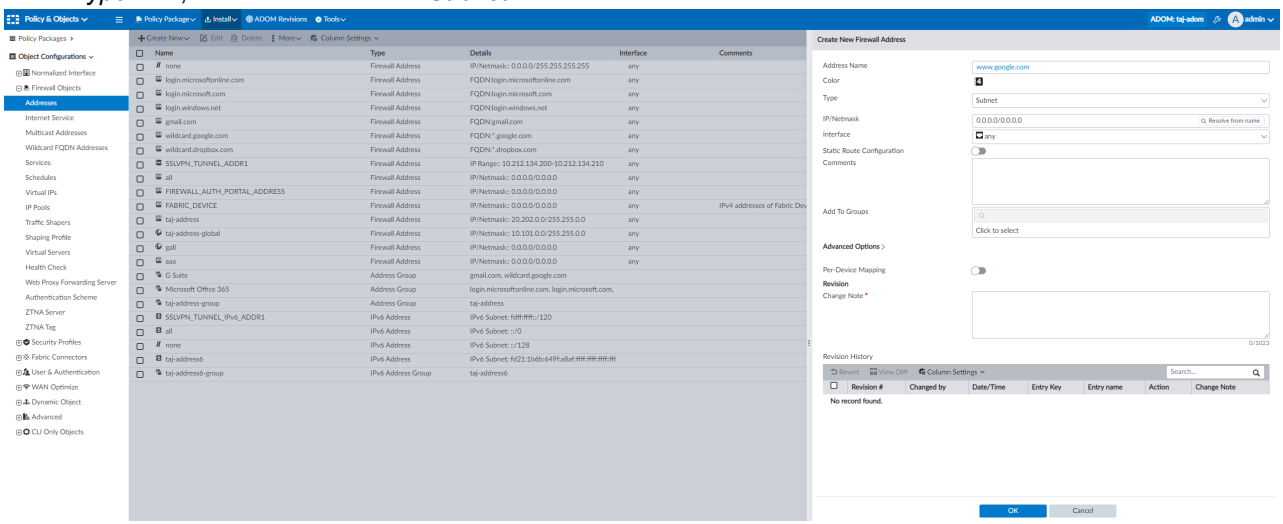
- FortiManager added support for FortiGate shared global objects 7.2.2 on page 193
- Object search is done using a persistent search menu, and the search extends to all object types 7.2.2 on page 199


## Resolve IP address from FQDN for firewall address type subnet

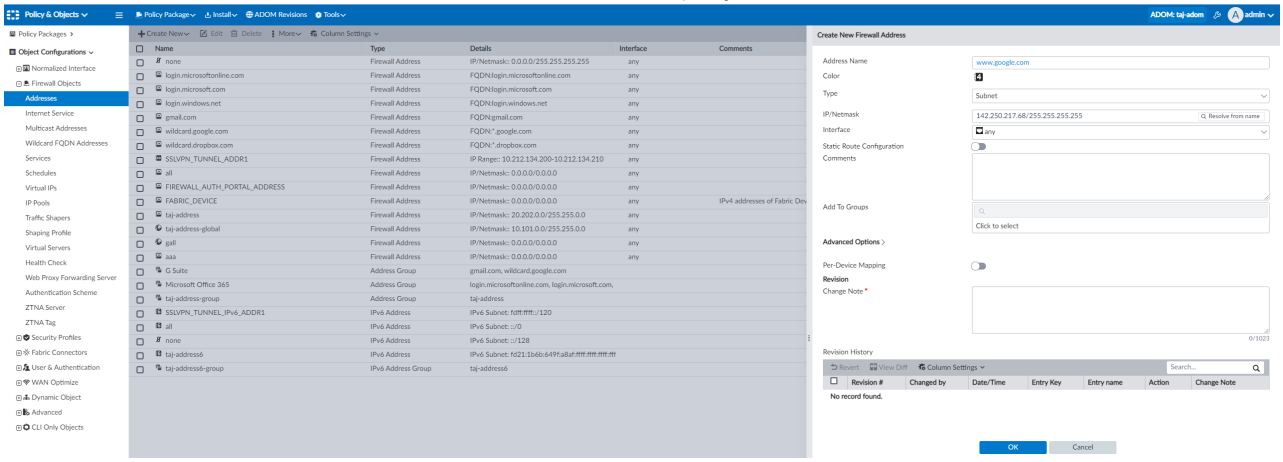
In FortiManager, you can resolve the IP address from the FQDN for "subnet" type firewall addresses.

**To resolve IP/Netmask from the FQDN in IPv4 address objects:**

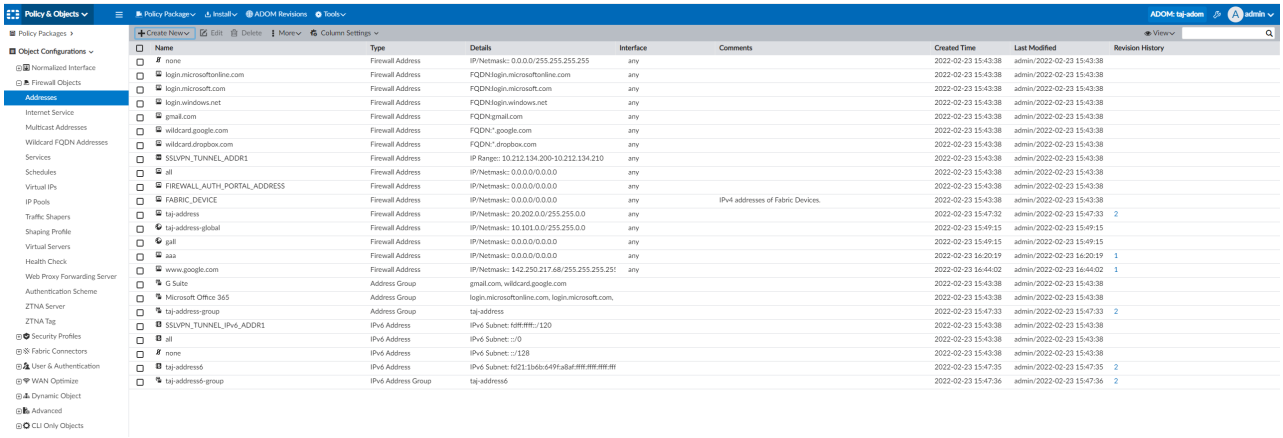
1. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Addresses*.
2. Create or edit a firewall address object.
3. In the *Address Name* field, enter the FQDN. For example, `www.google.com`.
4. In the *Type* field, leave the address as *Subnet*.



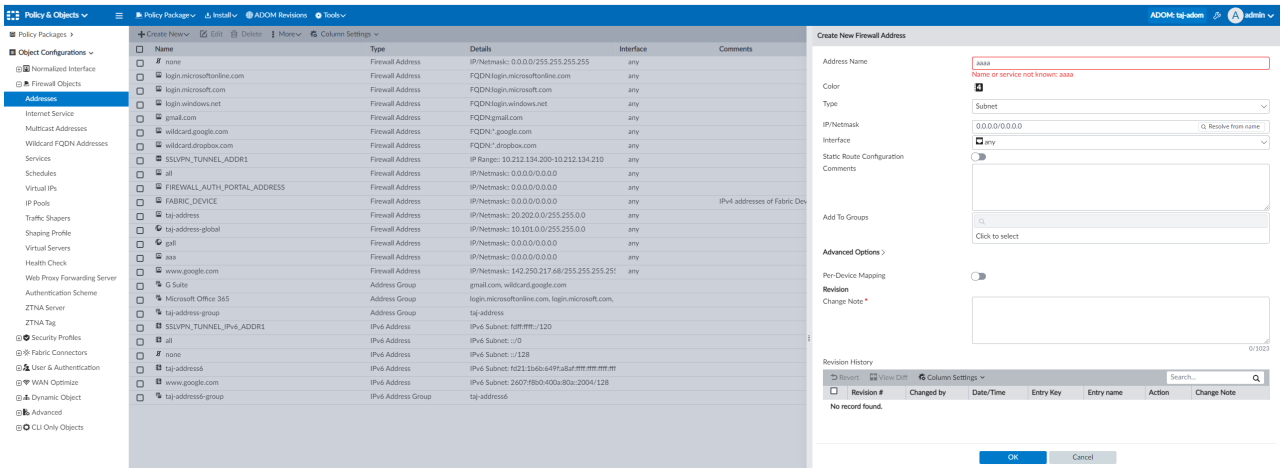

5. In the *IP/Netmask* field, click *Resolve from name*.
   The field is auto-filled with the first IP retrieved from the DNS query.



6. The saved address can be used in a policy.



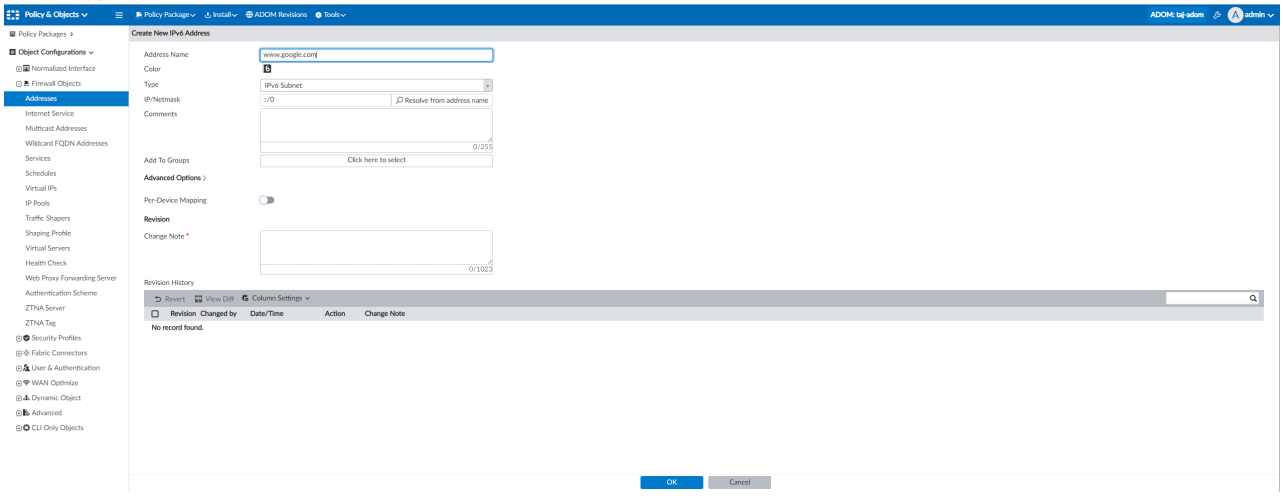
7. If FortiManager cannot resolve the host name/FQDN, the GUI will report the following error: `Name or service not known`.



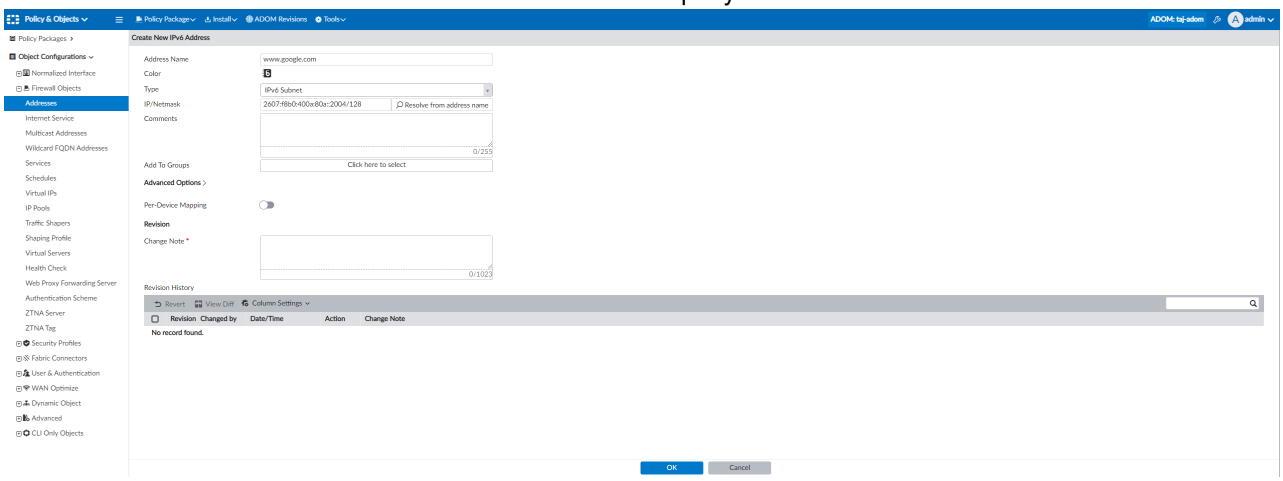
**To resolve IP/Netmask from the FQDN in IPv6 address objects:**

1. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Addresses*.
2. Create or edit a firewall address object.
3. In the *Address Name* field, enter the FQDN. For example, `www.google.com`.

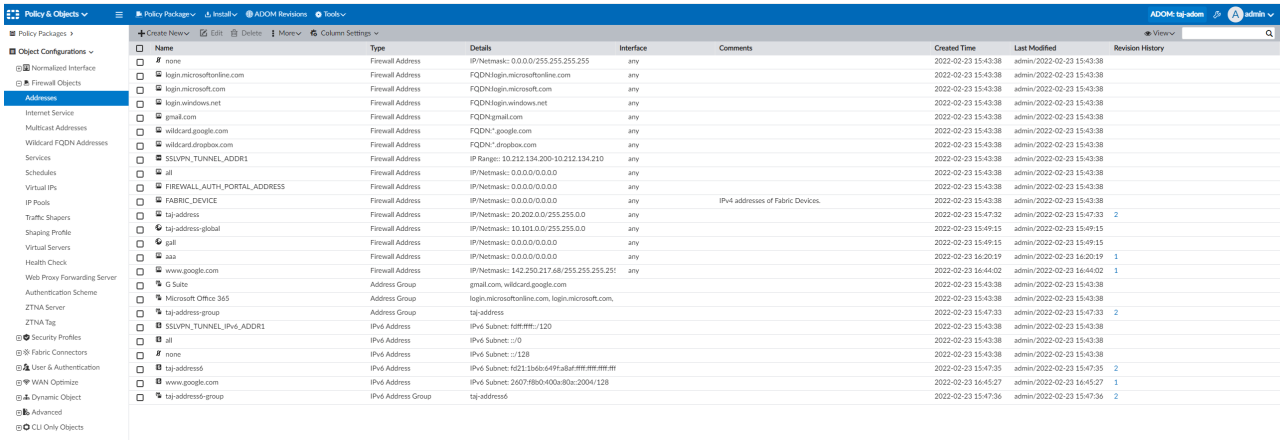
4. In the *Type* field, leave the address as *IPv6 Subnet*.




5. In the *IP/Netmask* field, click *Resolve from name*.
The field is auto-filled with the first IP retrieved from the DNS query.




6. The saved address can be used in a policy.

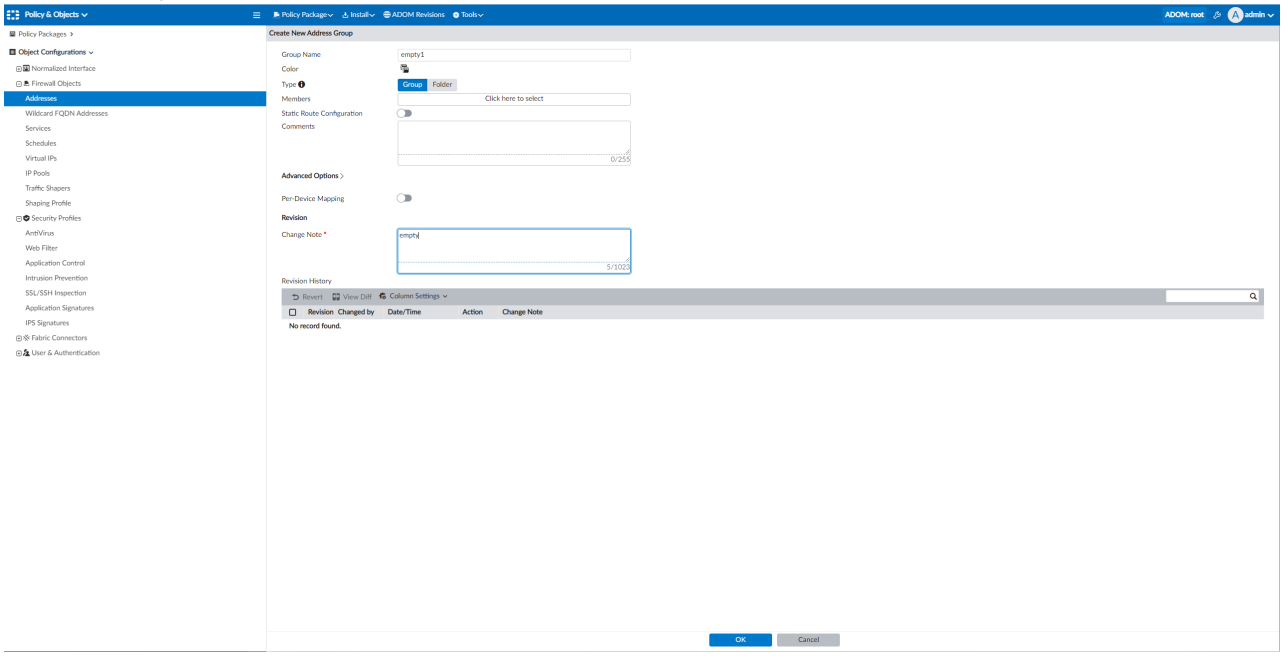


## FortiManager supports empty Address Group

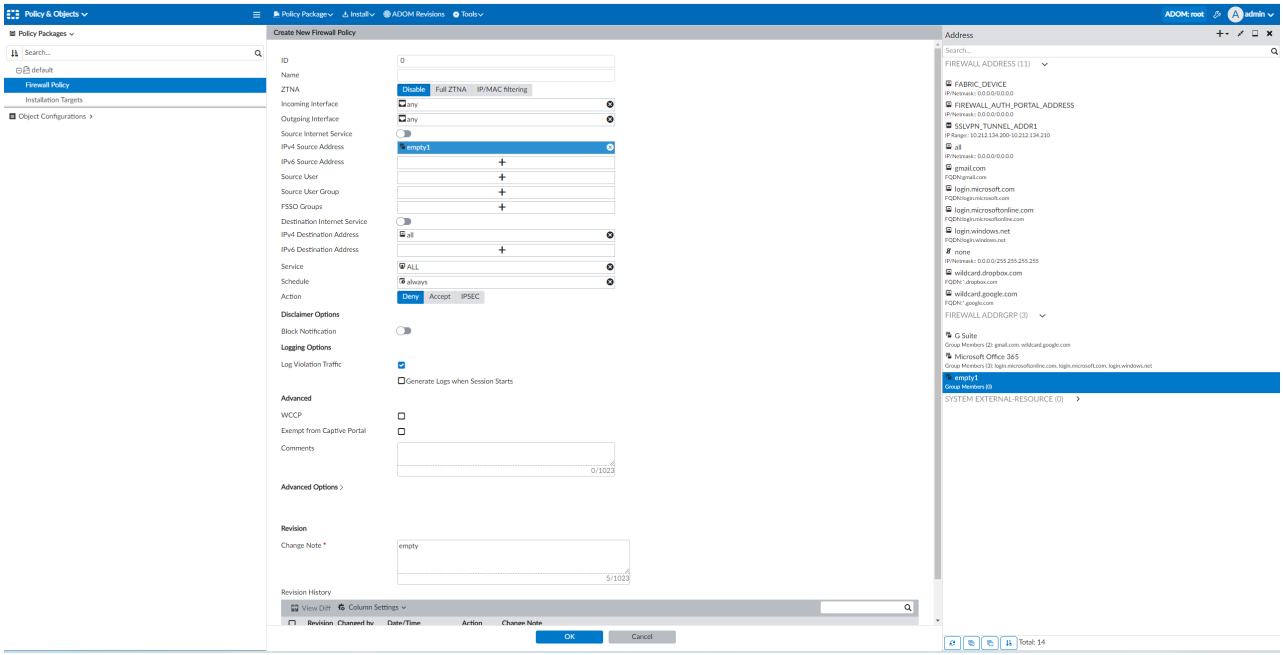
FortiManager supports creation of an empty Address Group that can be use in policies.

**To create a empty address group:**

1. Go to *Policy & Objects* > *Firewall Objects* > *Addresses*.
2. Create a new address group.
   Address Groups without members can be created.



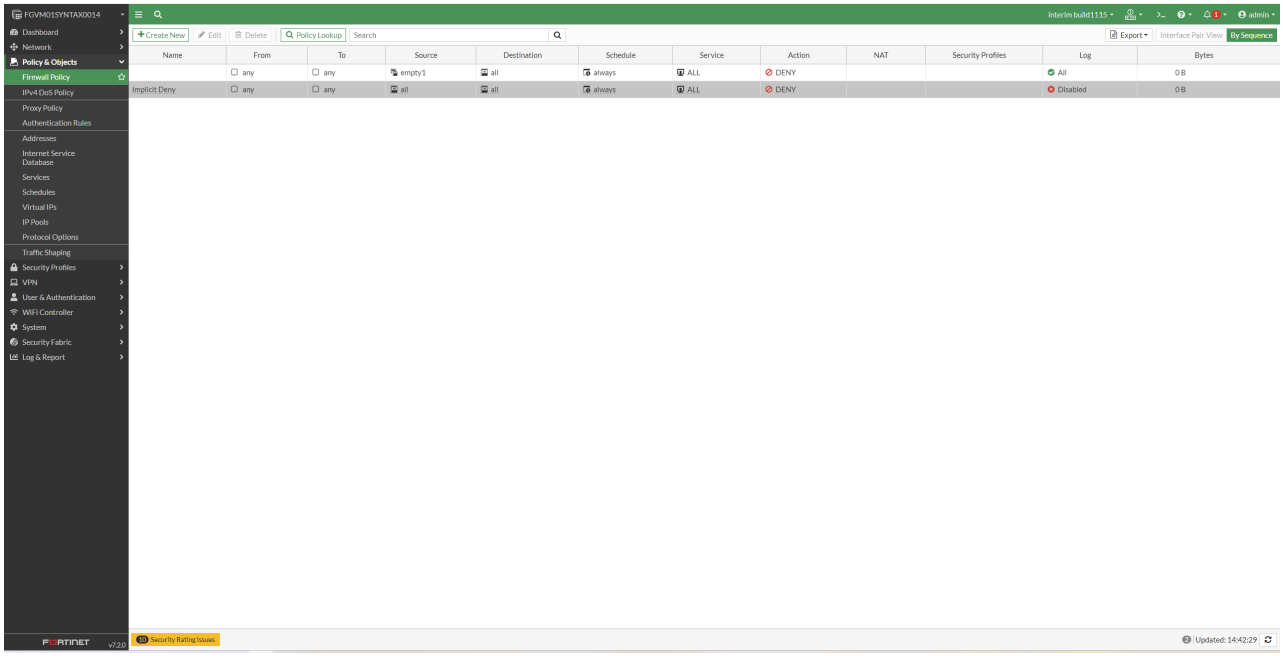

3. Create a policy which includes the empty Address Group.




4. Install the policy to a managed device.
   The empty address group is successfully installed.

```
config firewall addrgrp
   edit "empty1"
      set uuid (UUID)
      next
```

```
    end
  config firewall policy
    edit 1
      set uuid (UUID)
      set srcaddr "empty1"
      set dstaddr "all"
      set schedule "always"
      set service "ALL"
      next
    end
```

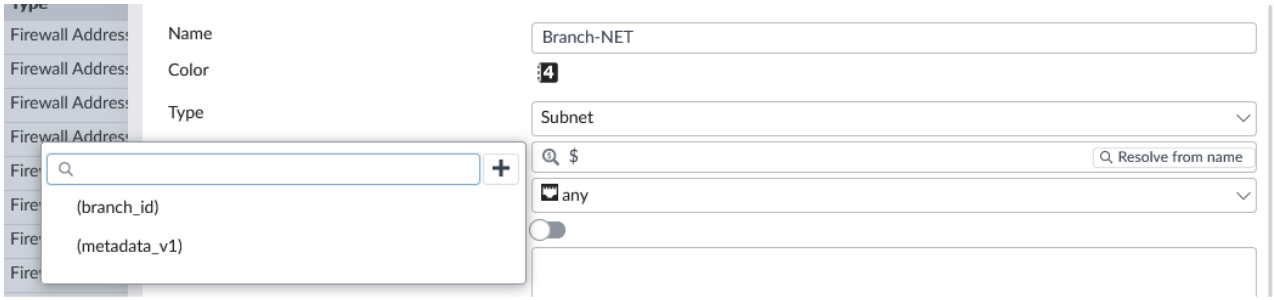



## Metadata Variables are supported in Firewall Objects configuration

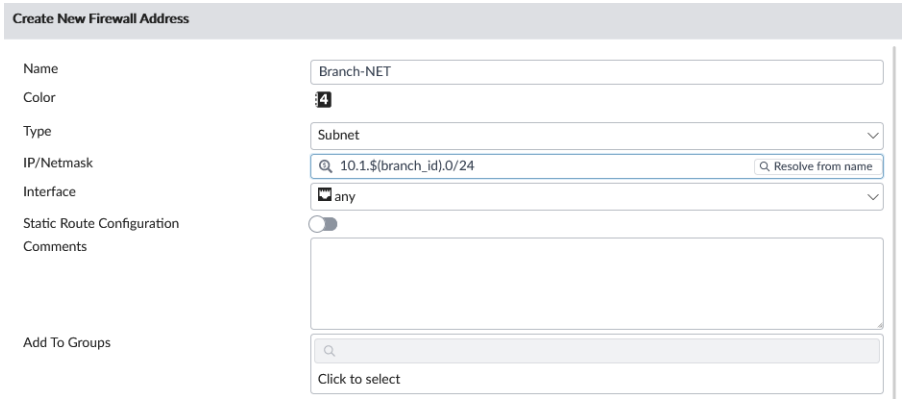
In FortiManager 7.2.0, metadata variables are supported in Firewall Objects configurations.

**To use a metadata variable in a dynamic objects:**

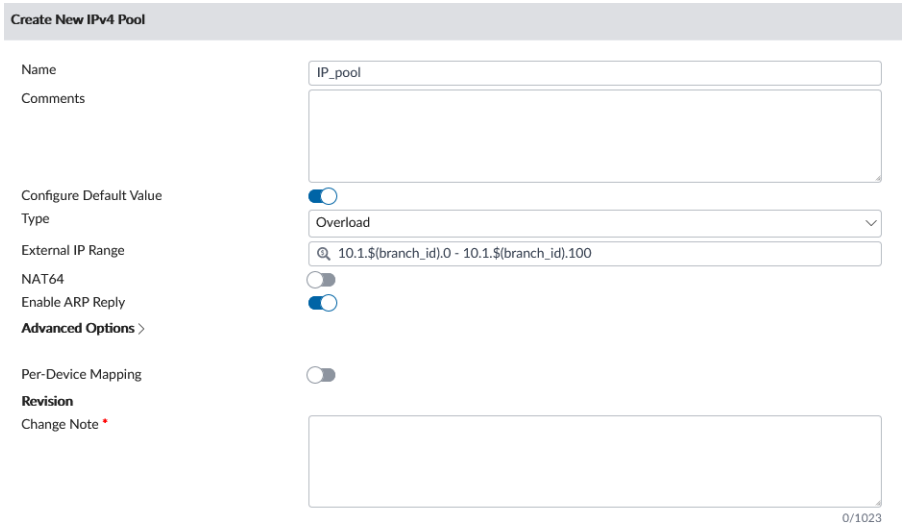
1. Go to *Policy & Objects* > *Object Configurations*.
2. Create or edit a firewall address, IP pool, or virtual IP.
3. Add the metadata in a supported text field using the following format: `$<metadata_variable_name>`.
   When `$` is typed into a supported text field, available metadata variables are displayed for selection. You can click the add button to create a new metadata variable.



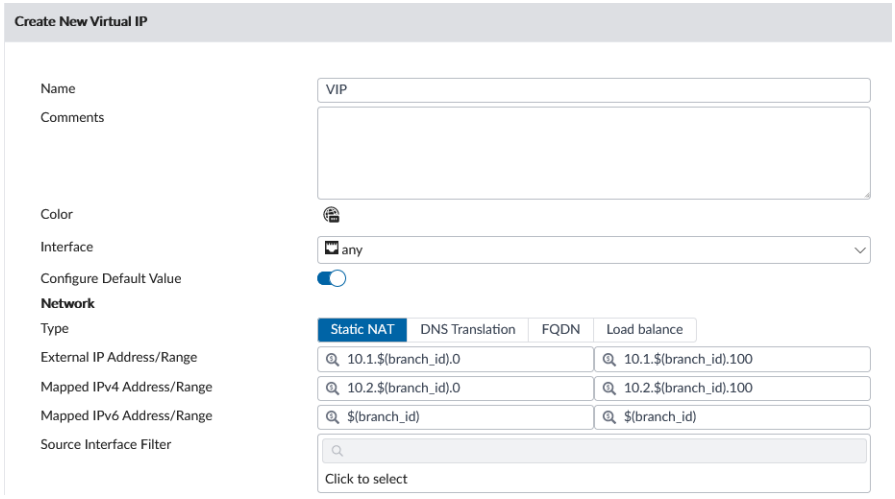
- For firewall addresses (subnet type), you can use metadata variables in the *IP/Netmask* field.




- For IP pools, you can use metadata variables in the *External IP Range* field.




- For virtual IPs, you can use metadata variables in the *External IP Address/Range*, *Mapped IPv4 Address/Range*, and *Mapped IPv6 Address/Range fields*.

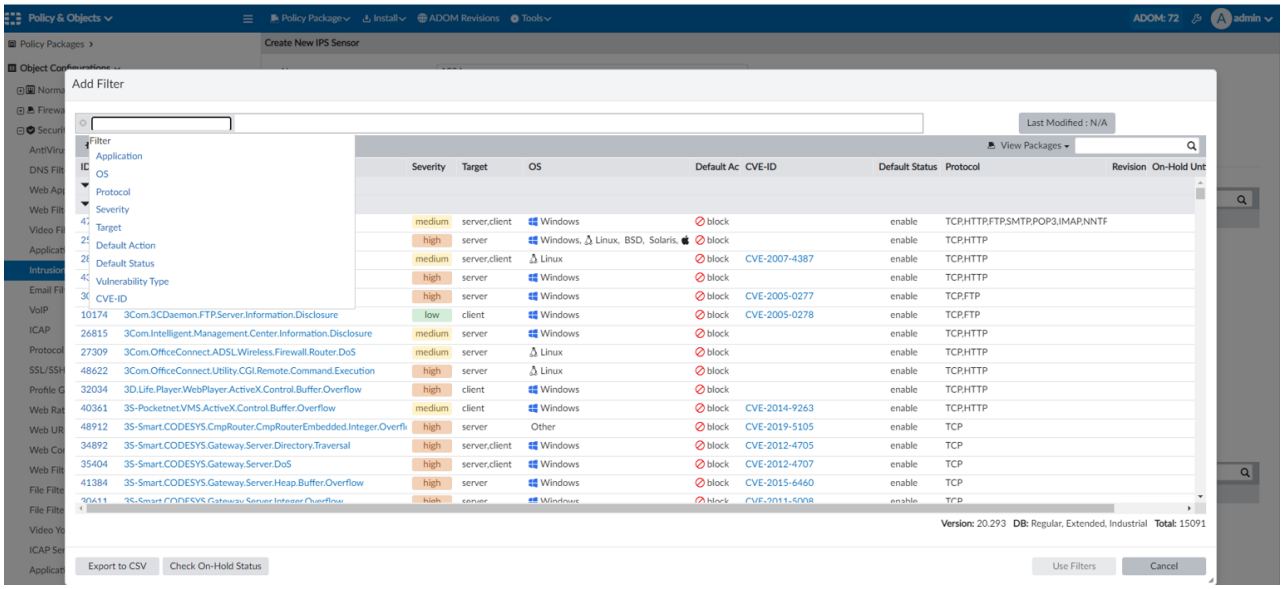


# Additional filters available for IPS sensors

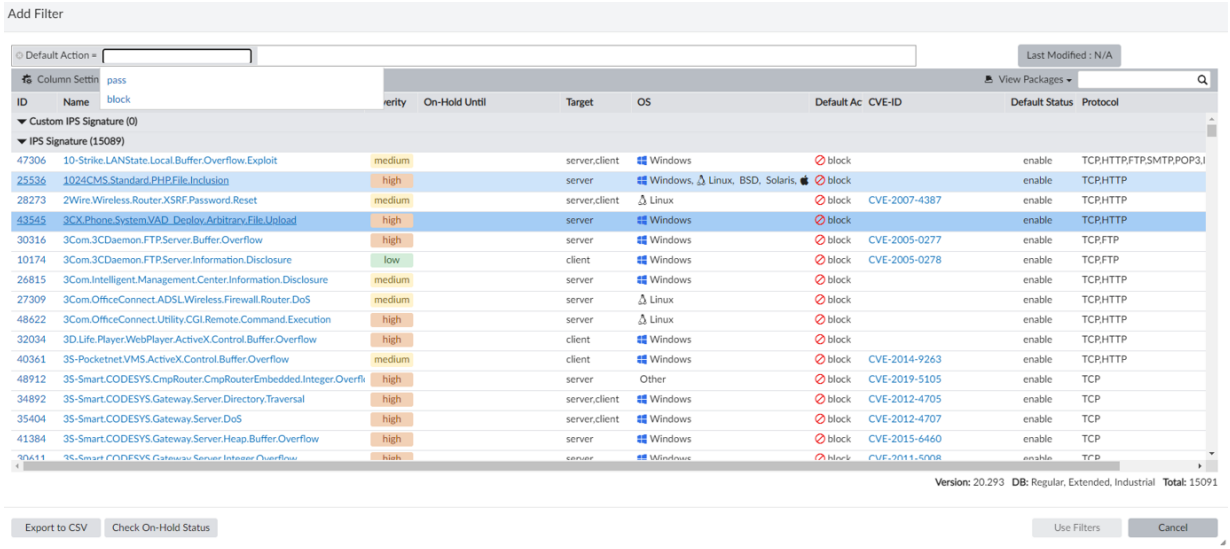
Users have more options to filter IPS signatures when configuring IPS sensor profiles. Signatures can be selected by these additional attributes: default status, default action, vulnerability type, and last update date.

**To filter by default action and default status:**

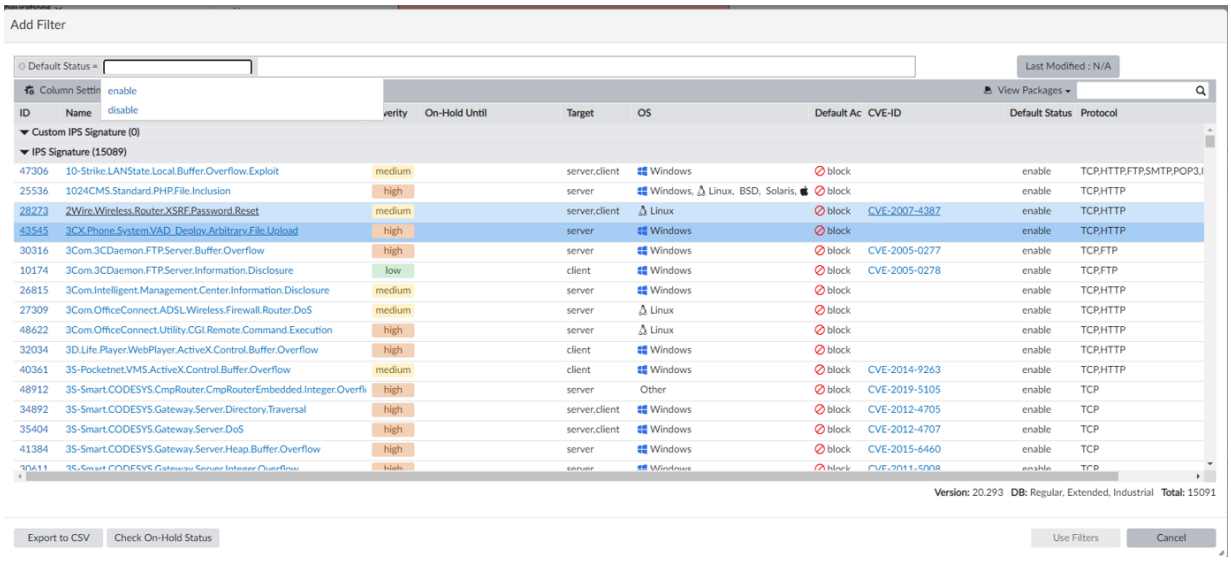
1. In FortiManager, edit an IPS sensor and add an IPS filter.
   Additional IPS filters are available including *Default Action*, *Default Status*, *Vulnerability Type*, and *Last Modified*.



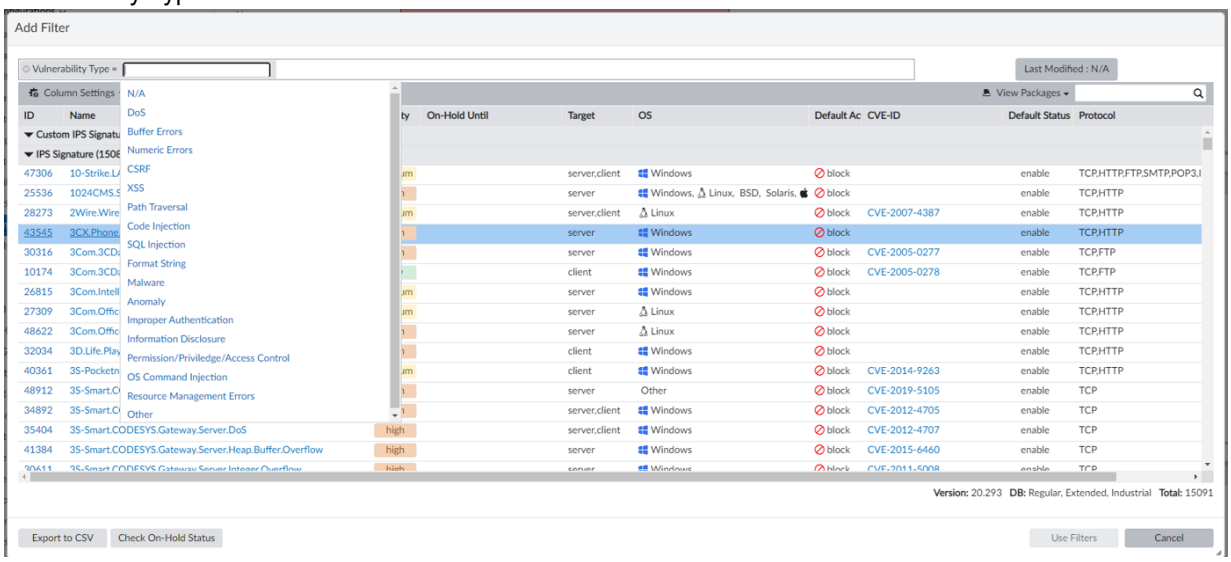

   a. Default Action



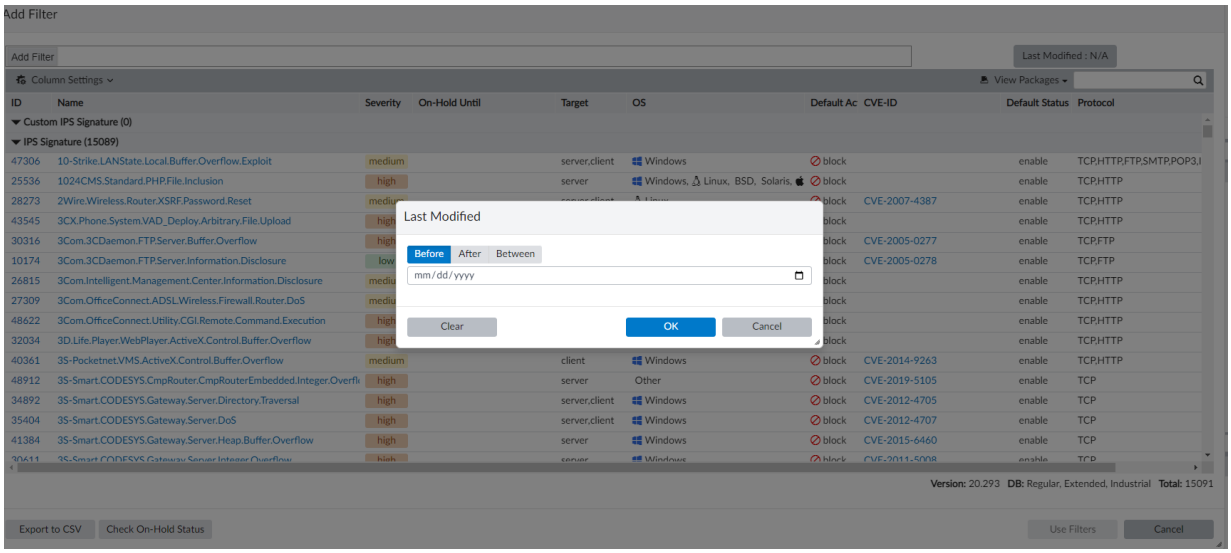
**b.** Default Status




**c.** Vulnerability Type



**d.** Last Modified

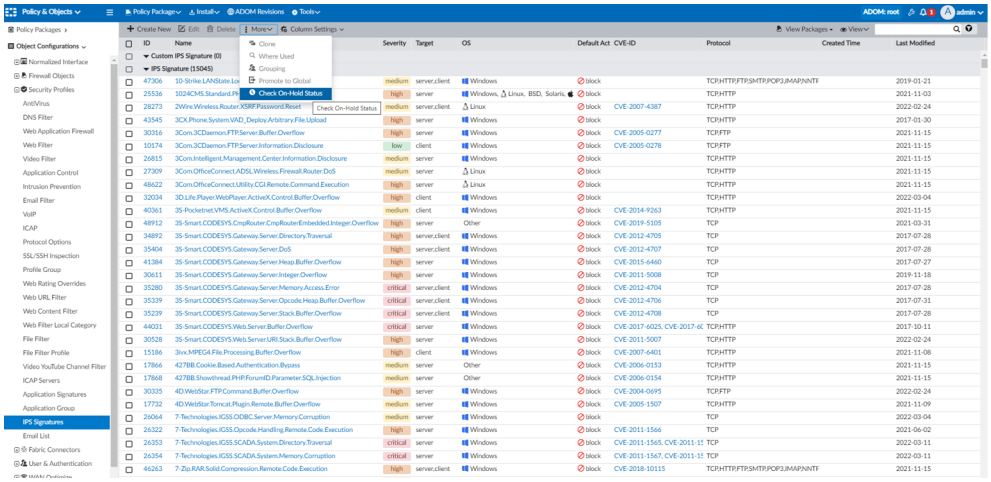



## Monitoring page for the IPS on-hold signatures

FortiManager 7.2.0 adds a monitoring page for the IPS on-hold signatures where you can check the on-hold status and show "On-Hold Until" information at the signature level.

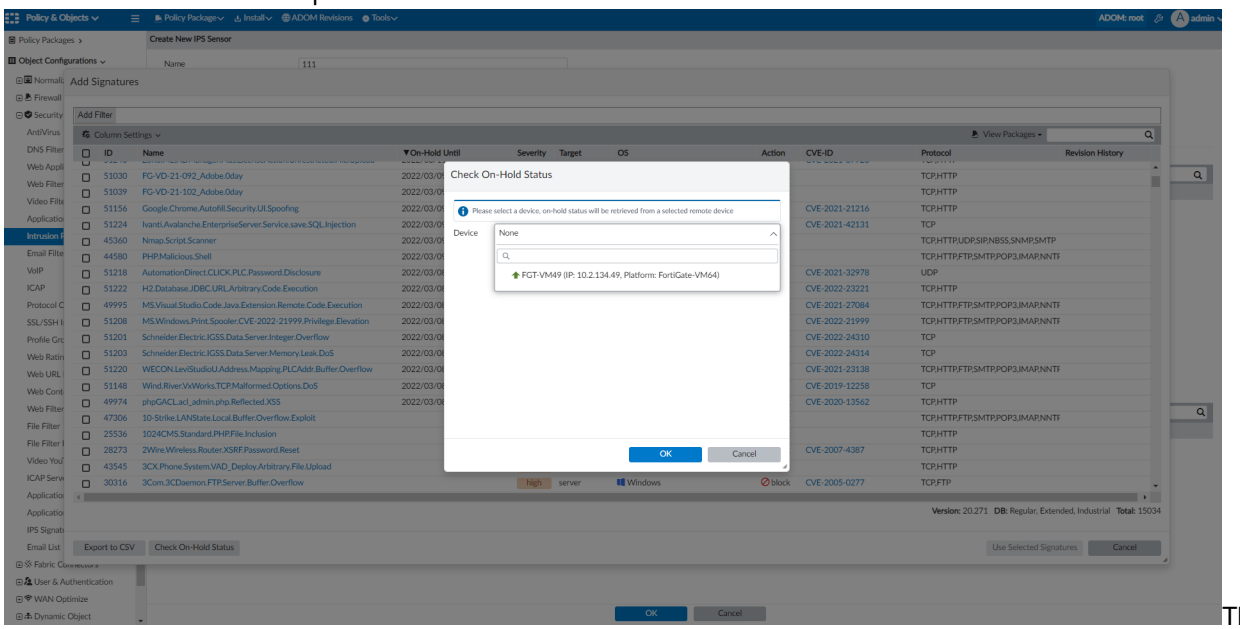
**To check the on-hold status:**

1. Go to *Policy & Objects* > *Object Configurations* > *Security Profiles* > *IPS Signatures*.
2. In the toolbar, select *More* > *Check On-Hold Status*.

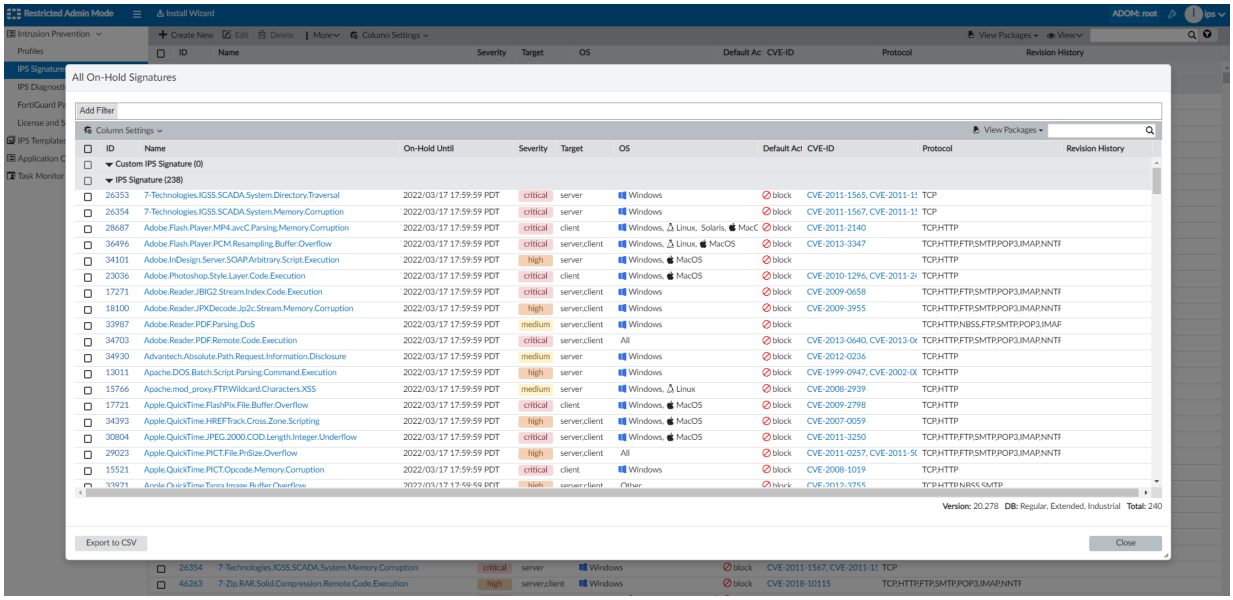



The *Check-On Hold Status* window appears.

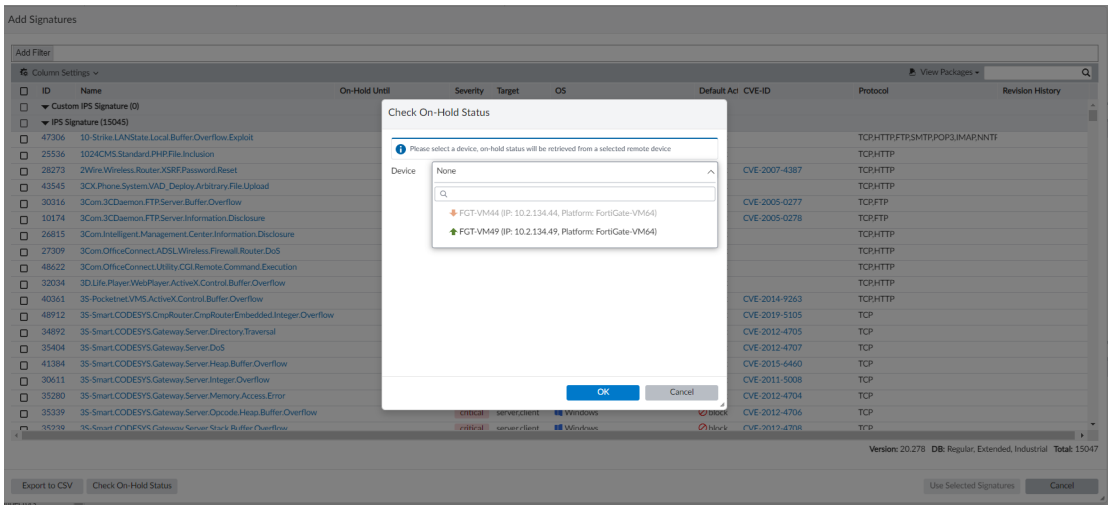
3. Select a device from the dropdown menu.




The *On-Hold Signatures* monitor is displayed. The date that signatures are held until is displayed in the *On-Hold Until* column.




The on-hold status can also be checked when creating a new IPS sensor.

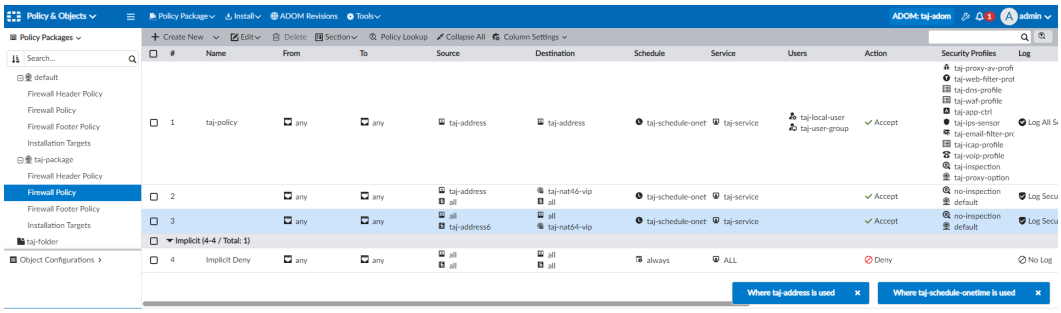



## Enhanced object "where used" function - 7.2.1

FortiManager includes an enhanced object "where used" function with multiple persistent where-used sessions and identification of single-object usage in the policy.

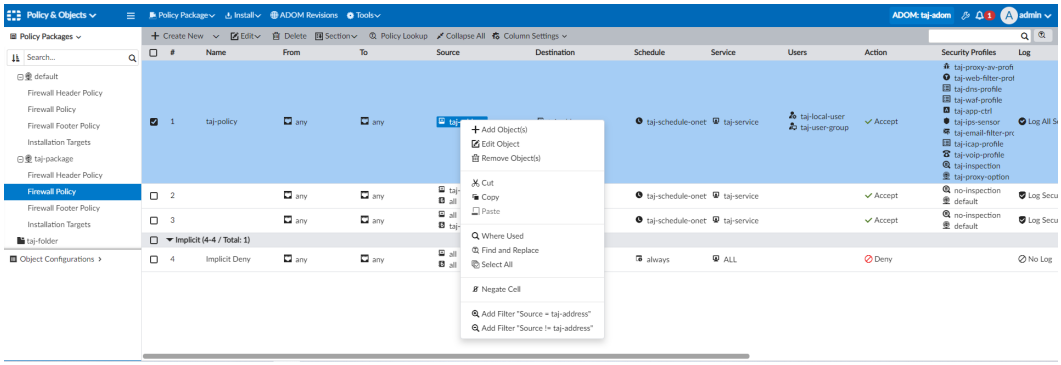
When using the *Where Used* function, you can view or edit rows without closing the *Where <x> is used* window. Instead, the *Where <x> is used* window stays open as a tab at the bottom right corner of the GUI. You can re-open or close the *Where <x> is used* window from this tab, as needed. Multiple *Where x is used* tabs are supported in the GUI.

For example, there are two *Where <x> is used* tabs available in the image below.



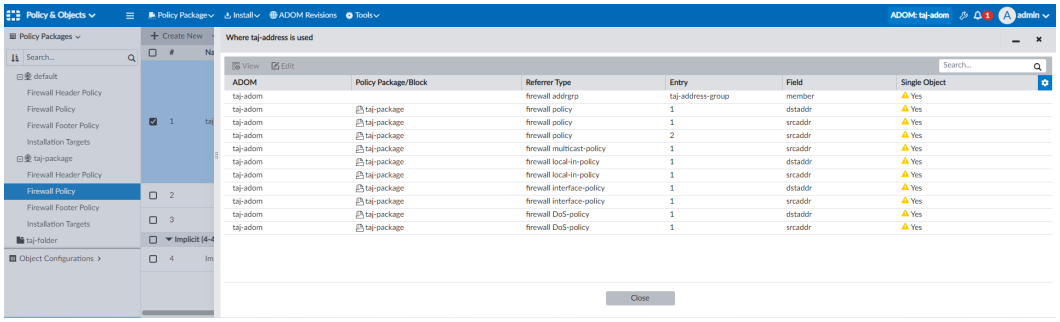
**To use the *Where Used* enhancement:**

1. Go to *Policy & Objects*.
2. Right-click an address and select *Where Used*.

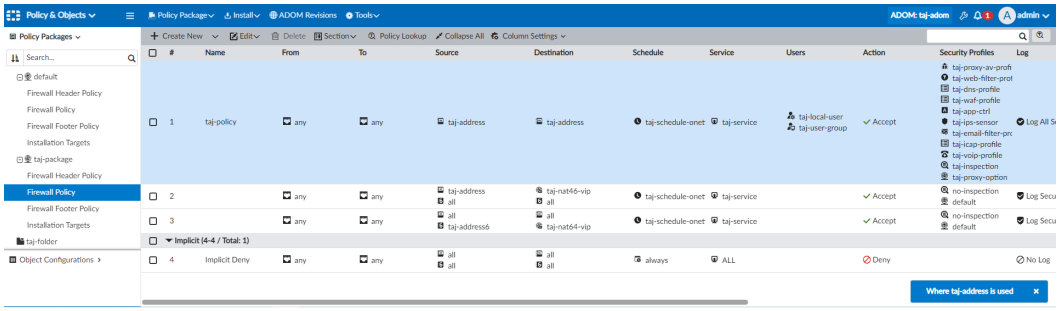



The *Where <x> is used* window displays.

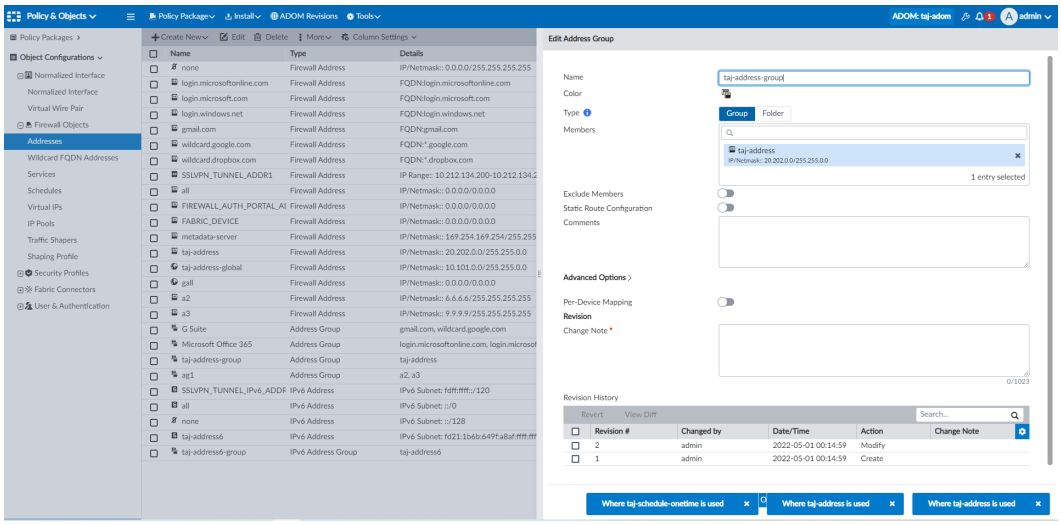
The *Single Object* column will be blank unless the address is the only object configured. If the address is the only object configured, the *Single Object* column will display *Yes*.




3. In the *Where <x> is used* window, click the minimize icon.
The *Where <x> is used* tab is now available in the bottom right corner of the GUI.




4. Click the title on the *Where <x> is used* tab to re-open the window.
5. In the *Where <x> is used* window, select a row and click *View* or *Edit*.
The *Where <x> is used* tab is available in the bottom right corner of the GUI while you view or edit the selection.
Note that the GUI supports multiple *Where <x> is used* tabs at the same time. See example below:



6. To close a *Where <x> is used* tab, click the *x* on the tab.

## Factory default firewall addresses and address group for private IP space (RFC1918) - 7.2.2

FortiManager includes factory default firewall addresses and address group for private IP space (RFC1918).

The following new default firewall addresses objects are available:

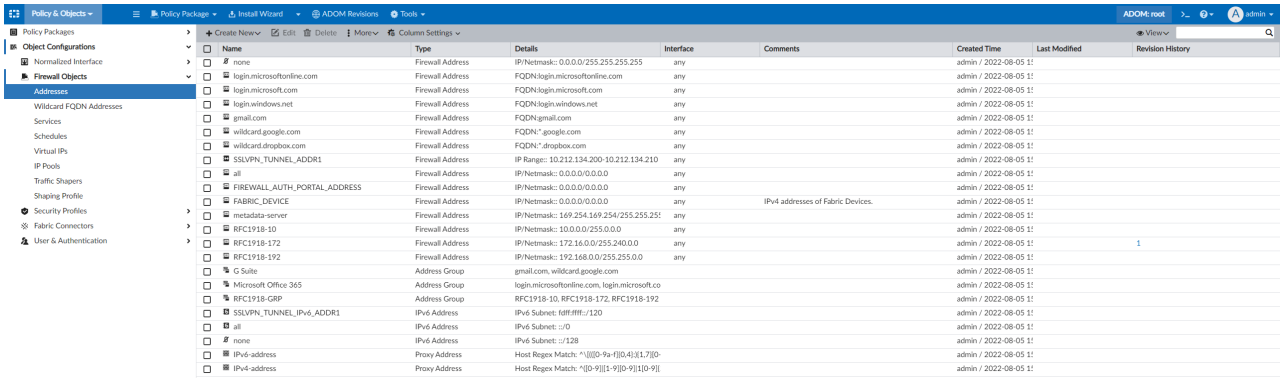
- **RFC1918-10**: 10.0.0/8
- **RFC1918-172**: 172.16.0.0/12
- **RFC1918-192**: 192.168.0.0/16

The following new default firewall address group is available:

- **RFC1918-GRP**: Includes the *RFC1918-10*, *RFC1918-172*, and *RFC1918-192* address objects.

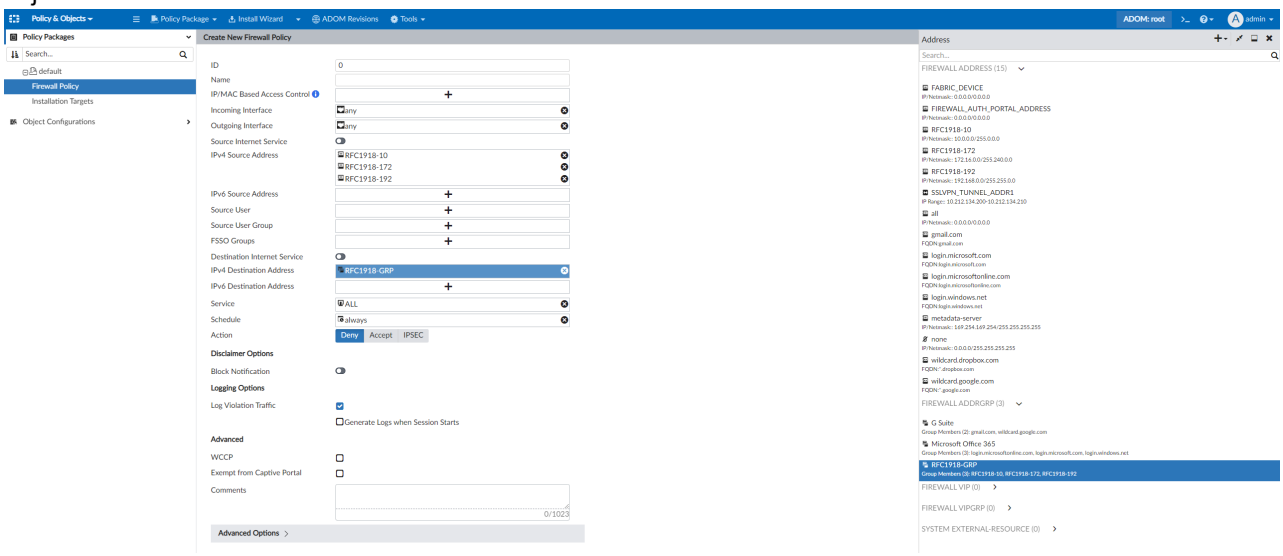
**To use the new default private IP space address objects in FortiManager:**

1. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Addresses*.
The default RFC1918 address objects are available.



2. Go to *Policy & Objects* > *Policy Packages*, and select a *Firewall Policy*.
You can select the firewall address objects for use in the policy. For example, the RFC1918-GRP address group

object is selectable as an IPv4 Destination Address.




3. Install the policy package to FortiGate.

**To edit the default private IP space address objects using the CLI:**

1. In the FortiManager CLI, use the config firewall address command.
   For example:

```
config firewall address
edit "RFC1918-10"
set subnet 10.0.0.0 255.0.0.0
next
edit "RFC1918-172"
set subnet 172.16.0.0 255.240.0.0
next
edit "RFC1918-192"
set subnet 192.168.0.0 255.255.0.0
next
end
config firewall addrgrp
edit "RFC1918-GRP"
set member "RFC1918-10" "RFC1918-172" "RFC1918-192"
next
end
```

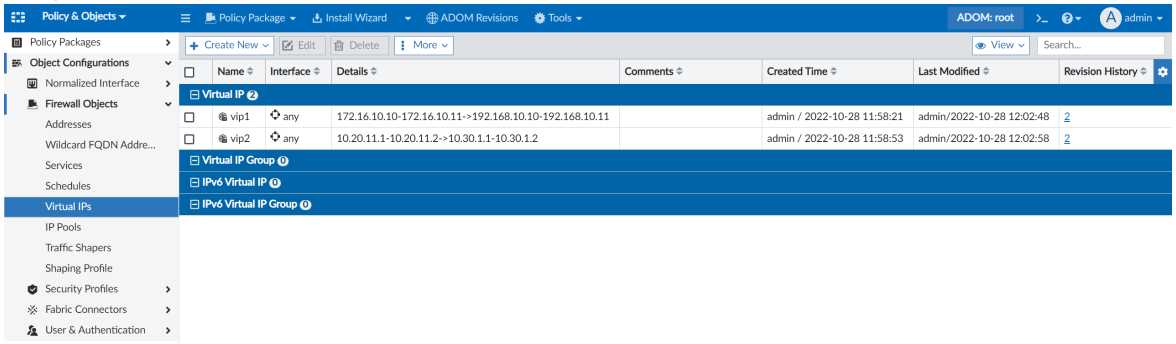
## Virtual IP (VIP) objects defined as an IP range are now searchable by an IP in the range - 7.2.2

Virtual IP (VIP) objects defined as an IP range are now searchable by an IP in the range.

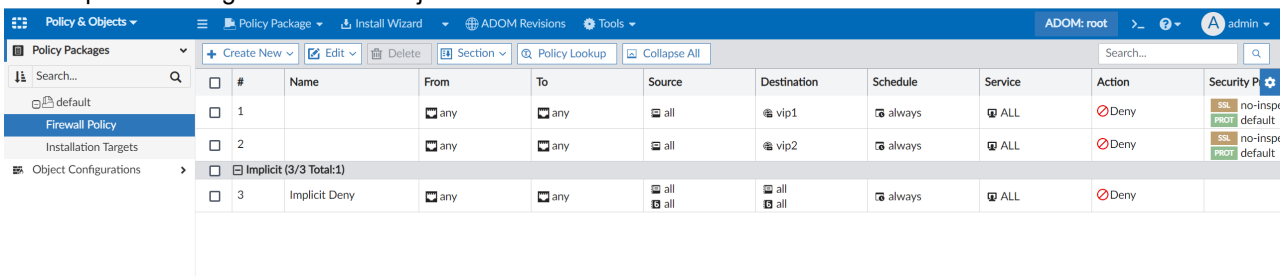
When searching for a VIP object by the first or last IP in the range, search results will return the VIP object in the search results using either *Simple* and *Strict* search.

**To search for Virtual IP ranges in policies:**

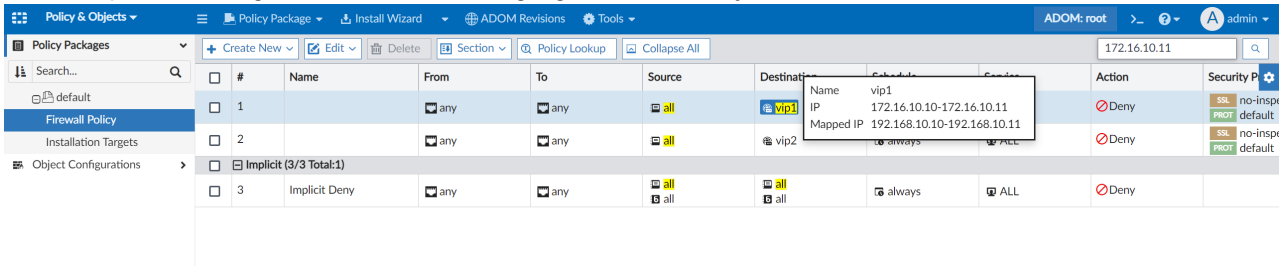
1. Create Virtual IP (VIP) objects.
   a. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Virtual IPs*.
   b. Click *Create New*, and create your Virtual IP address objects.
   In the example below, the following objects are created:
   - *vip1* with an *External IP Address Range* of `172.16.10.10` to `172.16.10.11` and a *Mapped IPv4 Address Range* of `192.168.10.10` to `192.168.10.11`.
   - *vip2* with an *External IP Address Range* of `10.20.11.1` to `10.20.11.2` and a *Mapped IPv4 Address Range* of `10.30.1.1` to `10.30.1.2`.



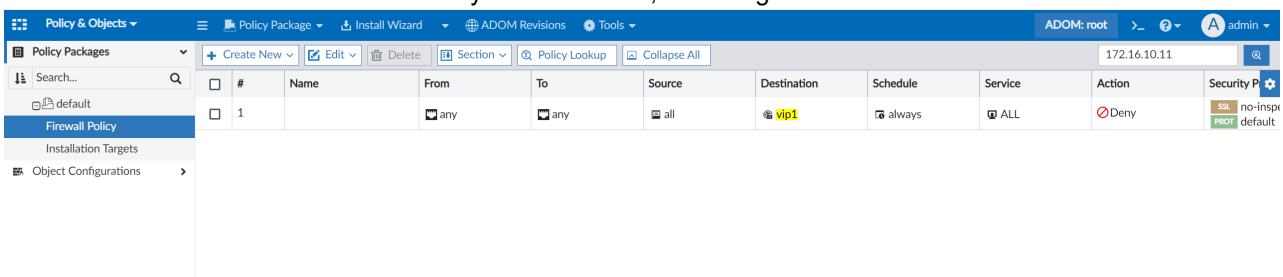

2. Create policies using the Virtual IP objects.




3. In the Firewall Policy search field, search for the first or last IP in the VIP range.
For example, searching for `172.16.10.11` highlights the VIP1 object in the search results.




You can also use Strict search to show only exact matches, excluding "all" results.



## FortiManager added support for FortiGate shared global objects - 7.2.2

FortiManager 7.2.2 supports the following FortiGate shared objects:

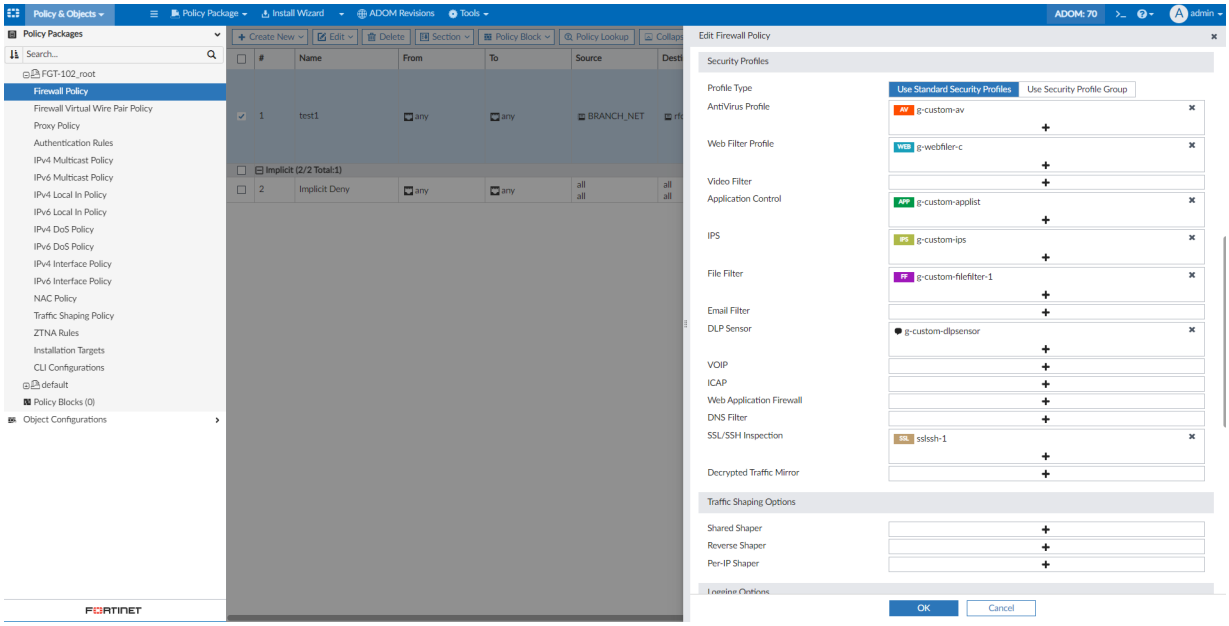
- system replacemsg-group
- system external-resource
- webfilter profile
- firewall wildcard-fqdn custom
- ips sensor
- sctp-filter profile
- application list
- dlp data-type
- dlp dictionary
- dlp sensor
- dlp profile
- webfilter search-engine
- antivirus profile
- file-filter profile
- wireless-controller utm-profile
- firewall ssh local-key
- firewall ssh local-ca

When global objects (starting with prefix g-) are referenced in a policy package, they are installed to the FortiGate Global VDOM and are usable in other VDOMs.

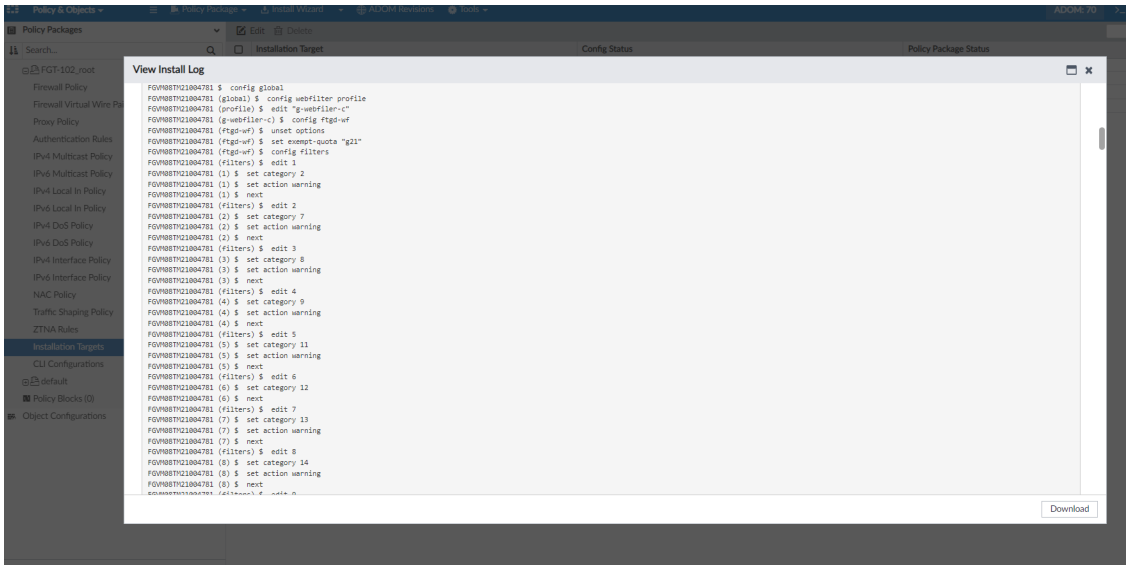
### Example of using shared objects

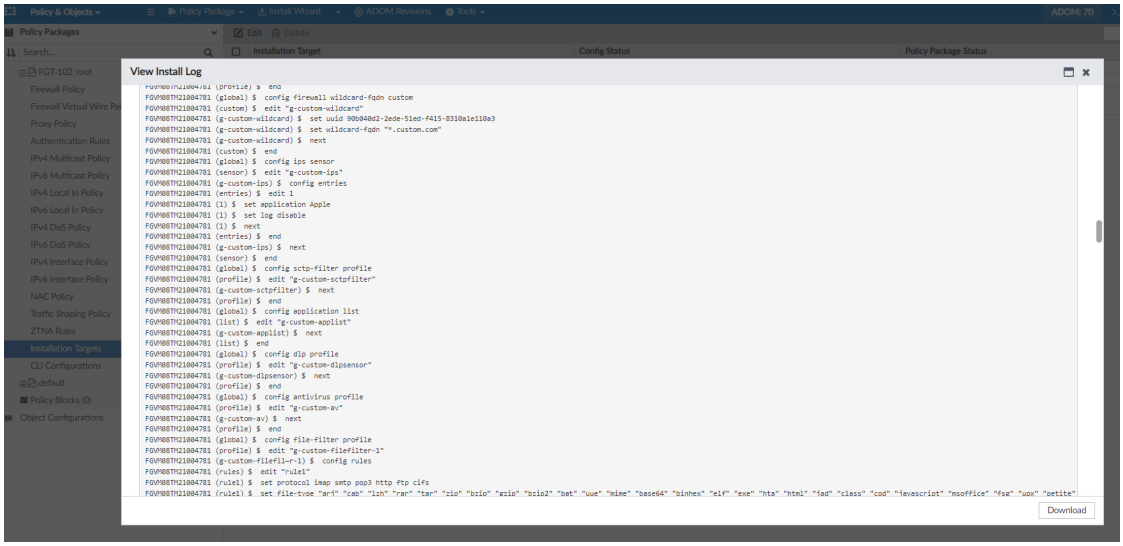
Following is an example of global objects (g-) being referenced in a policy package, and installed to a FortiGate:

- Shared objects are referenced in a policy package.

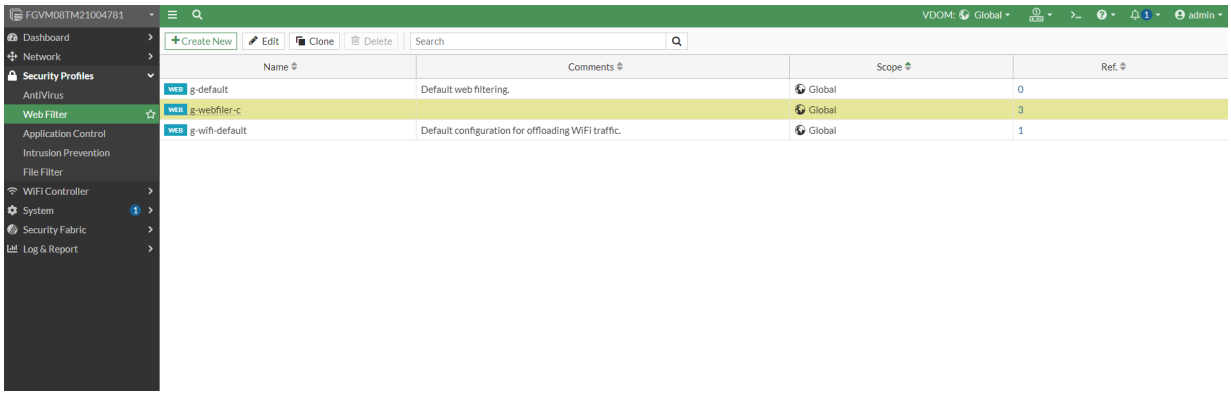


- The policy package is installed to FortiGate.

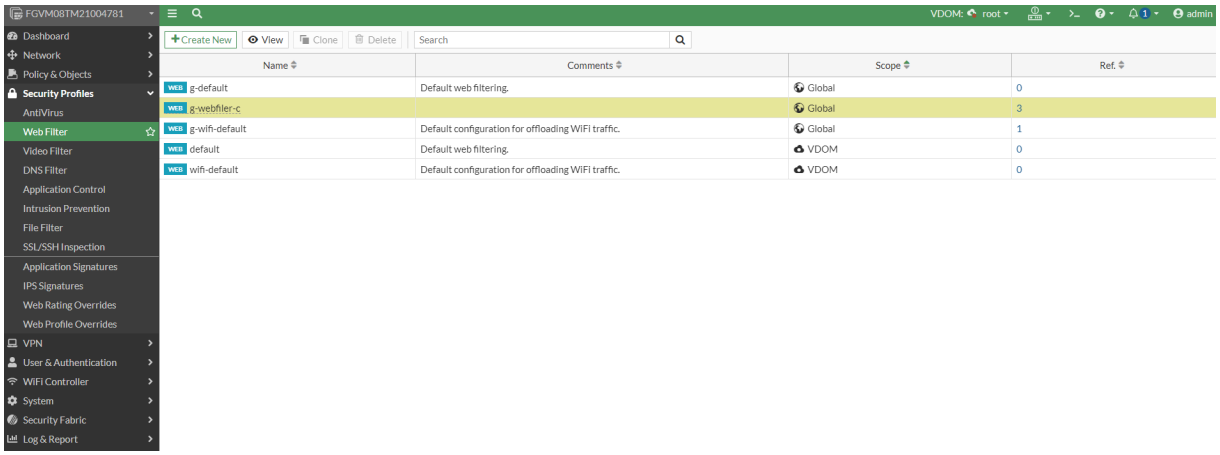



- Installation results in the creation of FortiGate global objects:



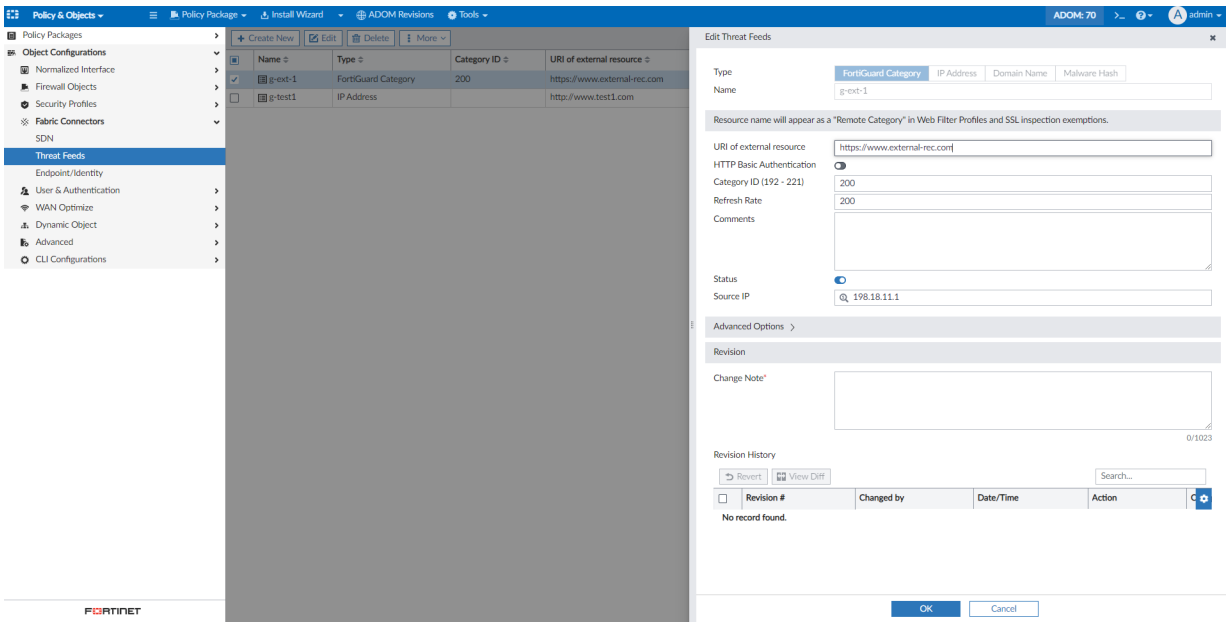
- Shared objects can be used by other VDOMs in the FortiGate.

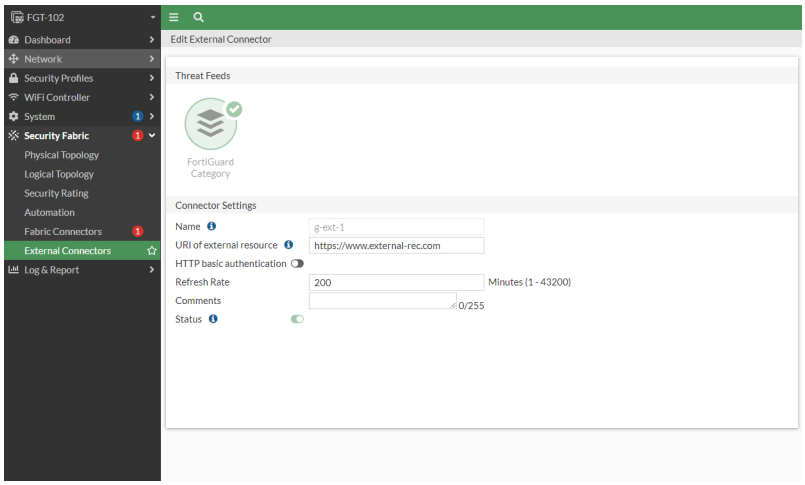



## Example objects

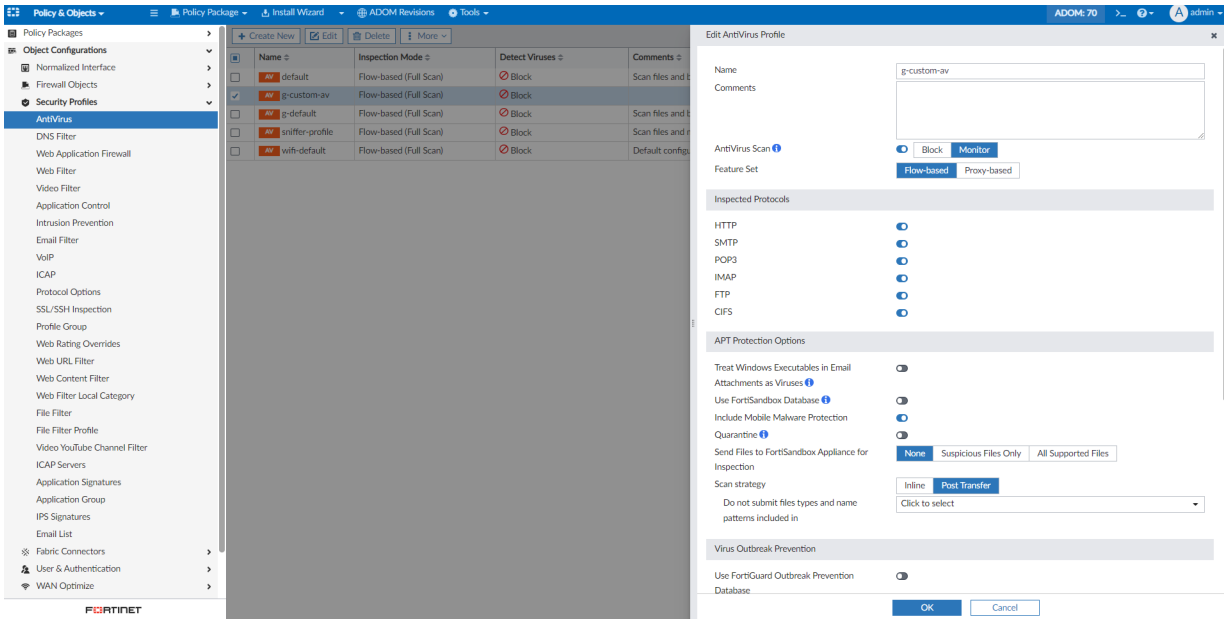
Following is an example of shared objects in both FortiManager and FortiGate. Once a shared object is created in FortiManager, the name of these objects cannot be changed.

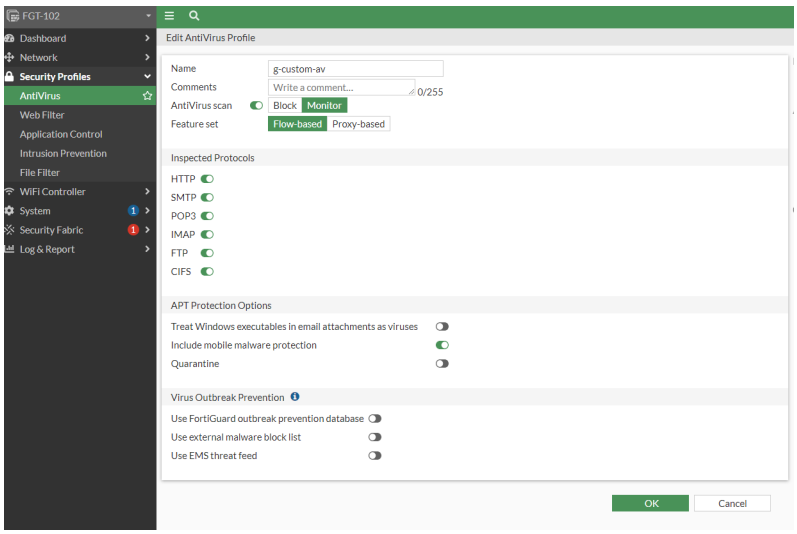
- External Resource



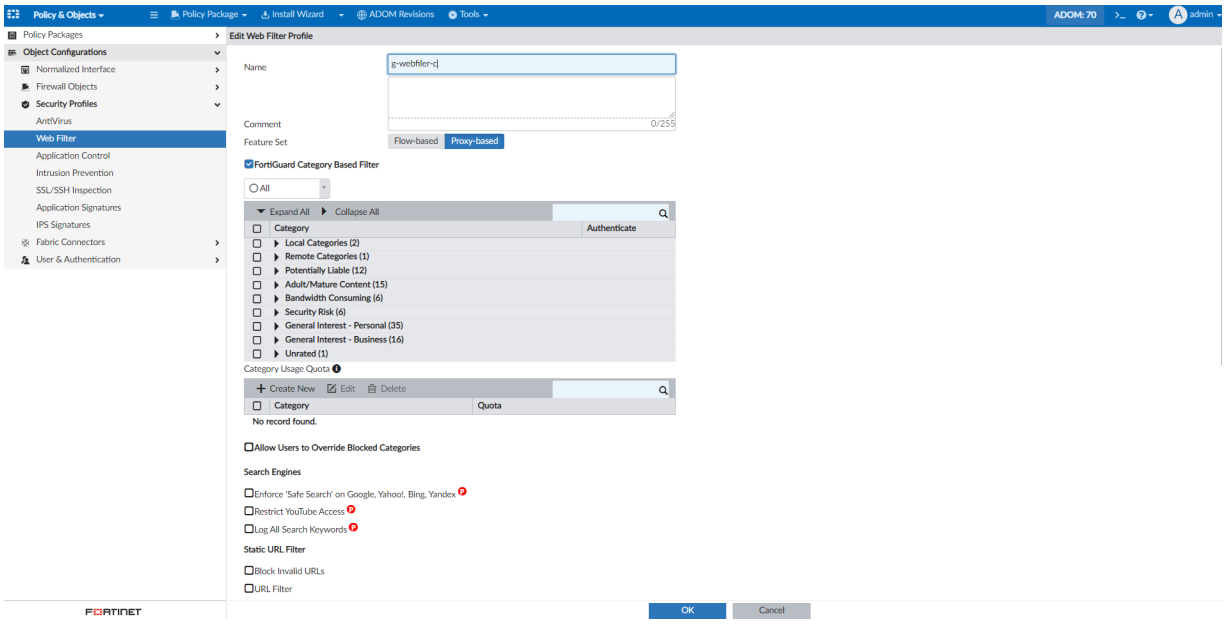

FGT-102
Dashboard
Network
Security Profiles
WiFi Controller
System
Security Fabric
Physical Topology
Logical Topology
Security Rating
Automation
Fabric Connectors
External Connectors
Log & Report
Edit External Connector
Threat Feeds
FortiGuard Category
Connector Settings
Name
g-ext-1
URI of external resource
https://www.external-rec.com
HTTP basic authentication
Refresh Rate
200
Minutes (1 - 43200)
Comments
0/255
Status

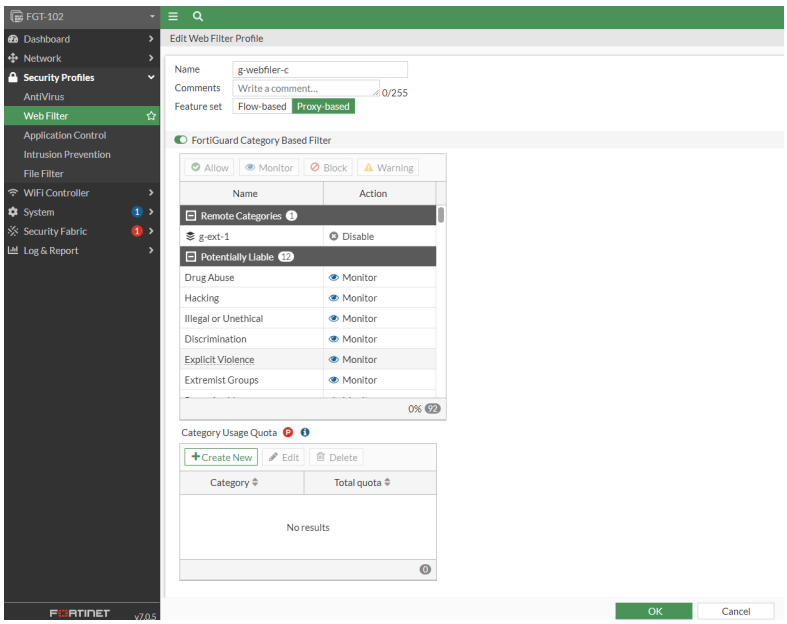
- AntiVirus


Policy & Objects
Policy Package
Install Wizard
ADOM Revisions
Tools
ADOM: 70
admin
Policy Packages
Object Configurations
Normalized Interface
Firewall Objects
Security Profiles
AntiVirus
DNS Filter
Web Application Firewall
Web Filter
Video Filter
Application Control
Intrusion Prevention
Email Filter
VoIP
ICAP
Protocol Options
SSL/SSH Inspection
Profile Group
Web Rating Overrides
Web URL Filter
Web Content Filter
Web Filter Local Category
File Filter
File Filter Profile
Video YouTube Channel Filter
ICAP Servers
Application Signatures
Application Group
IPS Signatures
Email List
Fabric Connectors
User & Authentication
WAN Optimize
Create New
Edit
Delete
More
Name
Inspection Mode
Detect Viruses
Comments
default
g-custom-av
g-default
sniffer-profile
wifi-default
Flow-based (Full Scan)
Block
Edit AntiVirus Profile
Name
g-custom-av
Comments
AntiVirus Scan
Block
Monitor
Feature Set
Flow-based
Proxy-based
Inspected Protocols
HTTP
SMTP
POP3
IMAP
FTP
CIFS
APT Protection Options
Treat Windows Executables in Email Attachments as Viruses
Use FortiSandbox Database
Include Mobile Malware Protection
Quarantine
Send Files to FortiSandbox Appliance for Inspection
None
Suspicious Files Only
All Supported Files
Scan strategy
Inline
Post Transfer
Do not submit files types and name patterns included in
Click to select
Virus Outbreak Prevention
Use FortiGuard Outbreak Prevention Database
OK
Cancel

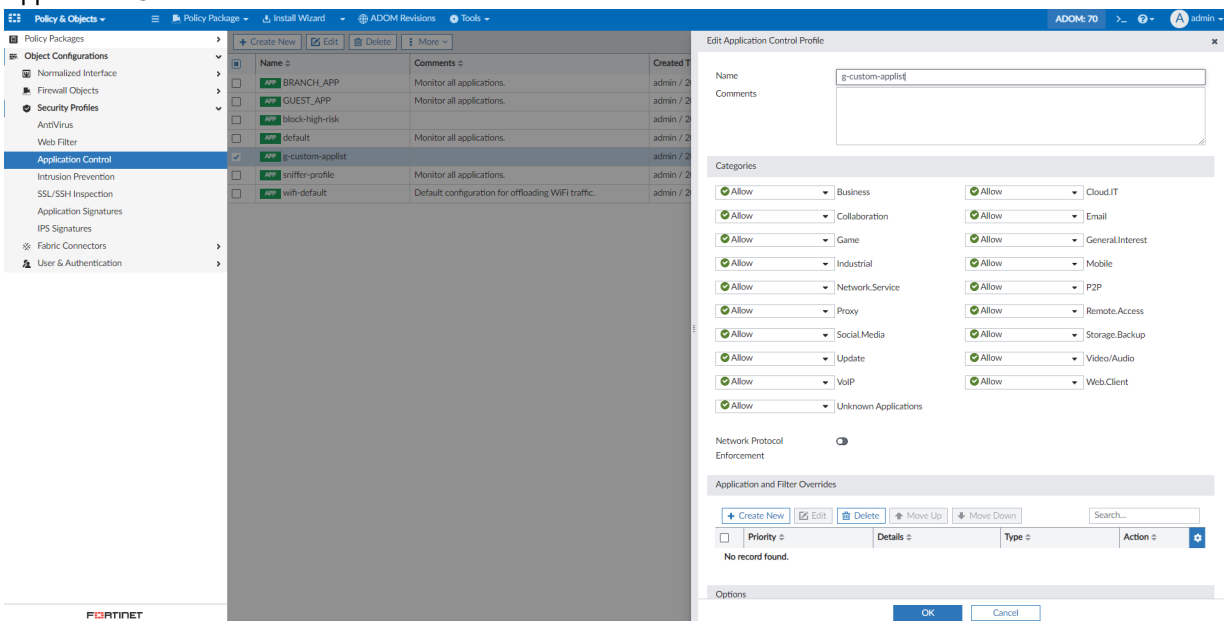

FGT-102
Dashboard
Network
Security Profiles
AntiVirus
Web Filter
Application Control
Intrusion Prevention
File Filter
WiFi Controller
System
Security Fabric
Log & Report
Edit AntiVirus Profile
Name
g-custom-av
Comments
Write a comment...
0/255
AntiVirus scan
Block
Monitor
Feature set
Flow-based
Proxy-based
Inspected Protocols
HTTP
SMTP
POP3
IMAP
FTP
CIFS
APT Protection Options
Treat Windows executables in email attachments as viruses
Include mobile malware protection
Quarantine
Virus Outbreak Prevention
Use FortiGuard outbreak prevention database
Use external malware block list
Use EMS threat feed
OK
Cancel

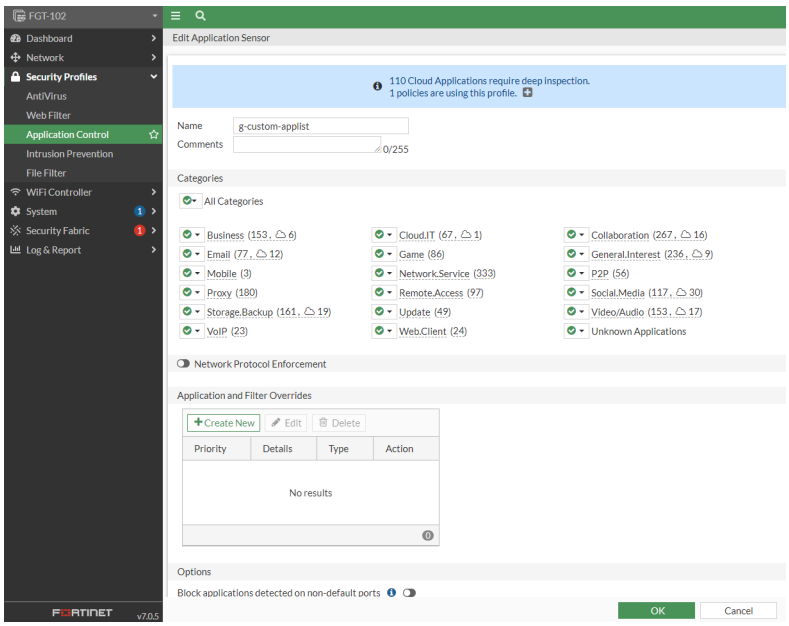
- Web Filter


Policy & Objects
Policy Package
Install Wizard
ADOM Revisions
Tools
ADOM: 70
admin
Policy Packages
Object Configurations
Normalized Interface
Firewall Objects
Security Profiles
AntiVirus
Web Filter
Application Control
Intrusion Prevention
SSL/SSH Inspection
Application Signatures
IPS Signatures
Fabric Connectors
User & Authentication
Edit Web Filter Profile
Name
g-webfiler-c
Comment
0/255
Feature Set
Flow-based
Proxy-based
FortiGuard Category Based Filter
All
Expand All
Collapse All
Category
Authenticate
Local Categories (2)
Remote Categories (1)
Potentially Liable (12)
Adult/Mature Content (15)
Bandwidth Consuming (6)
Security Risk (6)
General Interest - Personal (35)
General Interest - Business (16)
Unrated (1)
Category Usage Quota
Create New
Edit
Delete
Category
Quota
No record found.
Allow Users to Override Blocked Categories
Search Engines
Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex
Restrict YouTube Access
Log All Search Keywords
Static URL Filter
Block Invalid URLs
URL Filter
OK
Cancel

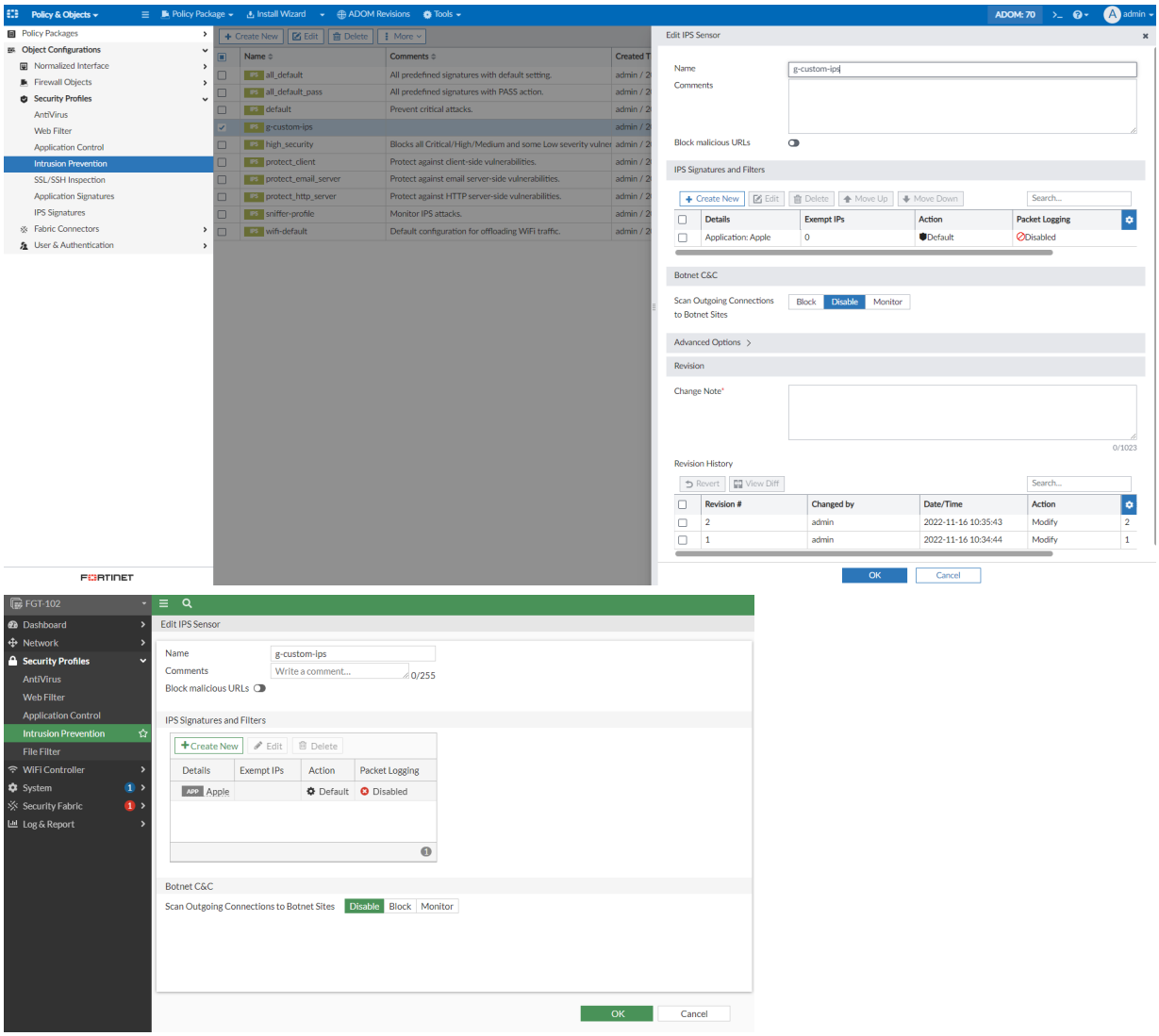

FGT-102
Dashboard
Network
Security Profiles
AntiVirus
Web Filter
Application Control
Intrusion Prevention
File Filter
WiFi Controller
System
Security Fabric
Log & Report
Edit Web Filter Profile
Name
g-webfiler-c
Comments
Write a comment...
0/255
Feature set
Flow-based
Proxy-based
FortiGuard Category Based Filter
Allow
Monitor
Block
Warning
Name
Action
Remote Categories
g-ext-1
Disable
Potentially Liable
Drug Abuse
Hacking
Illegal or Unethical
Discrimination
Explicit Violence
Extremist Groups
Monitor
0%
Category Usage Quota
Create New
Edit
Delete
Category
Total quota
No results
OK
Cancel

- Application Control



- Intrusion Prevention



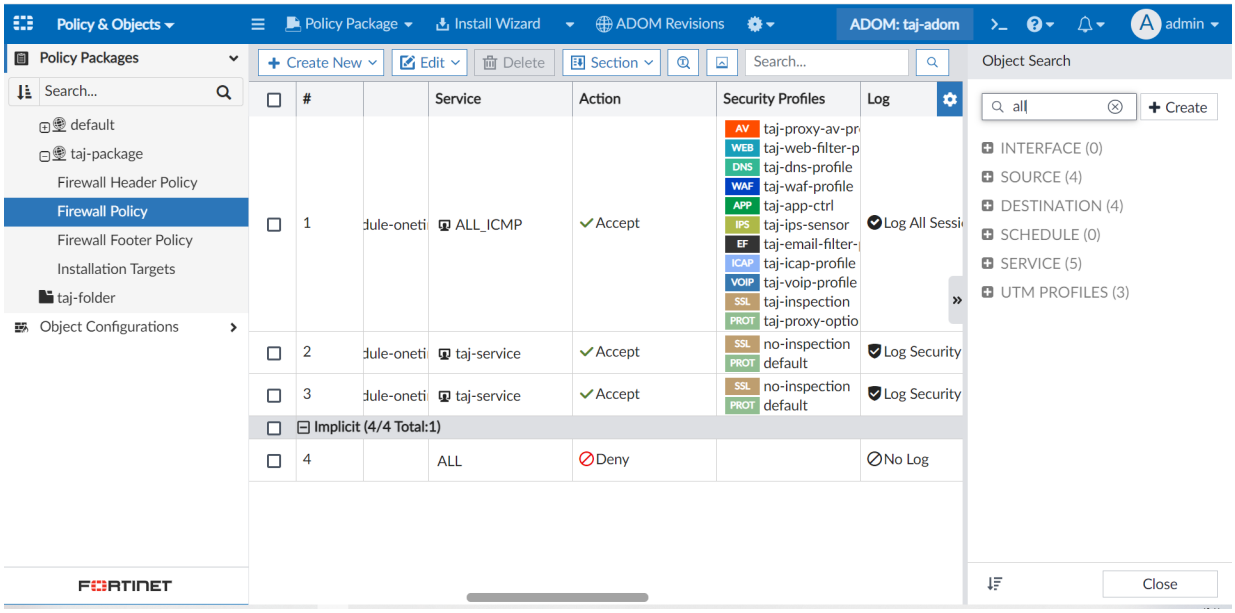

## Object search is done using a persistent search menu, and the search extends to all object types - 7.2.2

Object search is done using a persistent search menu, and the search extends to all object types.

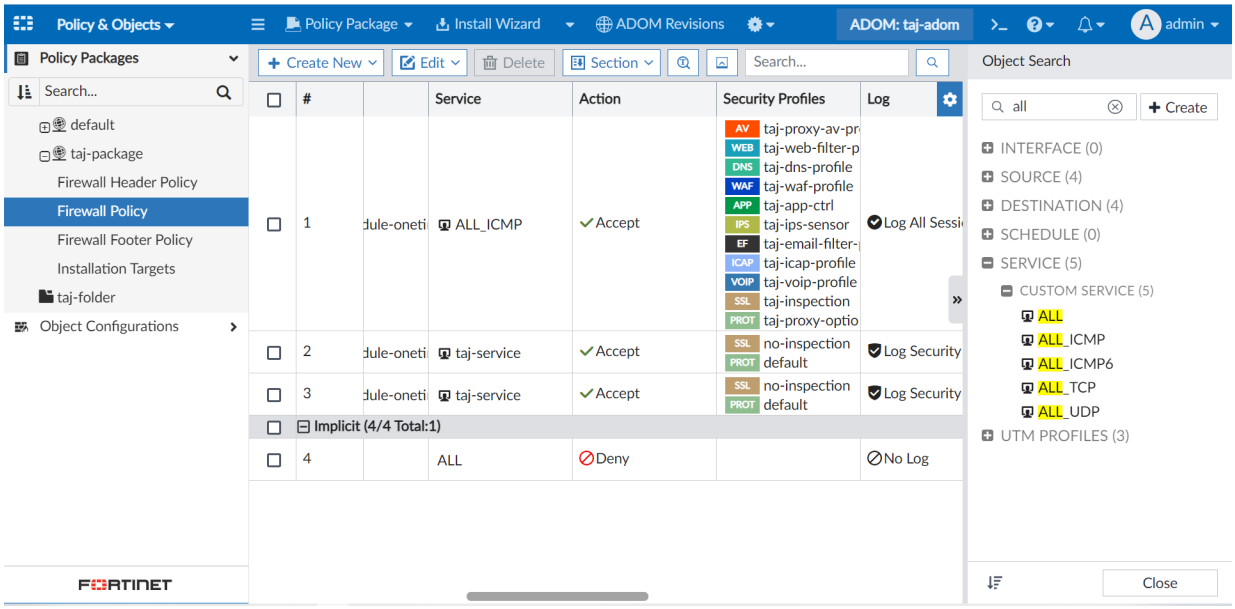
**To use the persistent search menu to search objects:**

1. Go to *Policy & Objects* > *Policy Packages* and select a policy.
2. In the policy table, users can click the double arrow icon (  ) to open the *Object Search* panel, and search for objects.

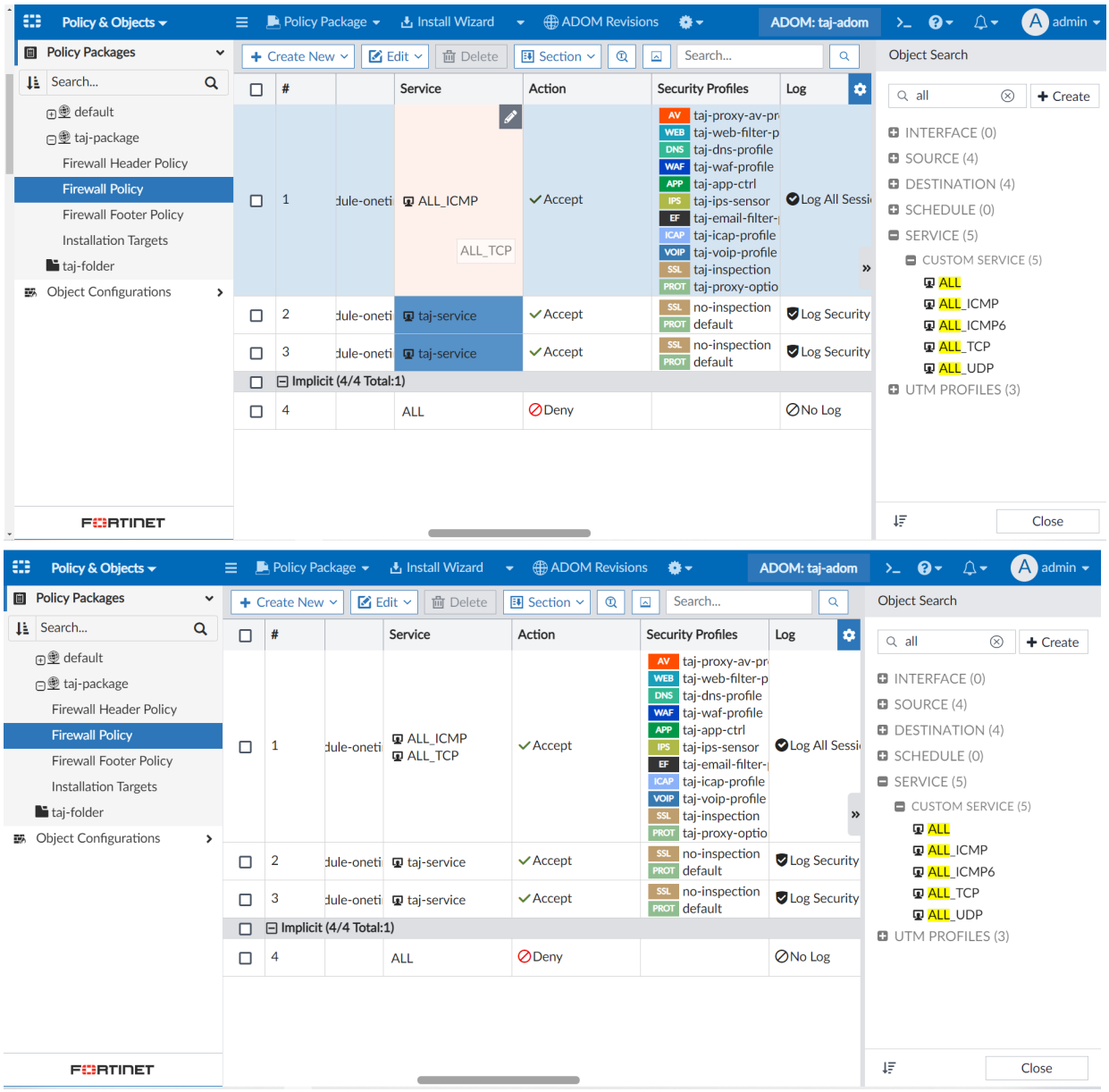
You can also create or edit existing objects from the *Object Search* panel.




3. From the search results, you can see which objects are configurable to which policy fields.




4. Users can assign objects from the search panel to a policy by dragging and dropping the object into the corresponding column. FortiManager only supports the drag-and-drop object feature when the object is placed in the column of the came category. In the example below, the *ALL_TCP Service* object is drag-and-dropped into the *Service* column for the policy.


Policy & Objects
Policy Package
Install Wizard
ADOM Revisions
ADOM: taj-adom
admin
Policy Packages
Search...
default
taj-package
Firewall Header Policy
Firewall Policy
Firewall Footer Policy
Installation Targets
taj-folder
Object Configurations
Create New
Edit
Delete
Section
Search...
Service
Action
Security Profiles
Log
1
ALL_ICMP
ALL_TCP
Accept
Log All Sessi
2
taj-service
Accept
no-inspection
default
Log Security
3
taj-service
Accept
no-inspection
default
Log Security
Implicit (4/4 Total:1)
4
ALL
Deny
No Log
Object Search
all
Create
INTERFACE (0)
SOURCE (4)
DESTINATION (4)
SCHEDULE (0)
SERVICE (5)
CUSTOM SERVICE (5)
ALL
ALL_ICMP
ALL_ICMP6
ALL_TCP
ALL_UDP
UTM PROFILES (3)
Close
FORTINET

# Fabric View

This section lists the new features added to FortiManager for Fabric View:



## Connectors

This section lists the new features added to FortiManager for connectors:

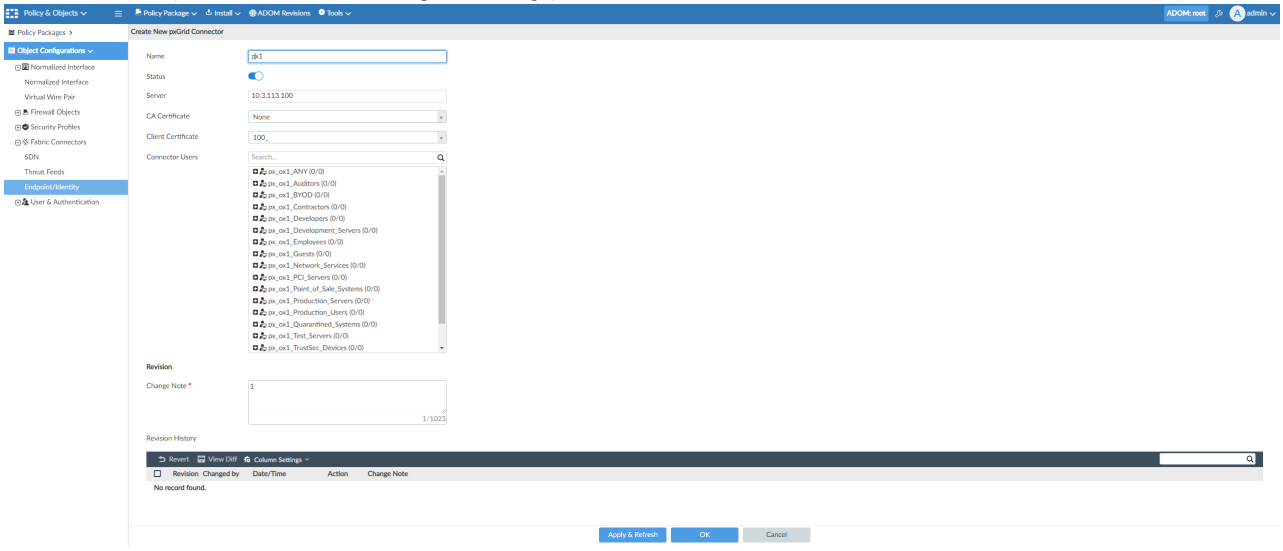


### Allow multiple Cisco PxGrid connectors in the same ADOM

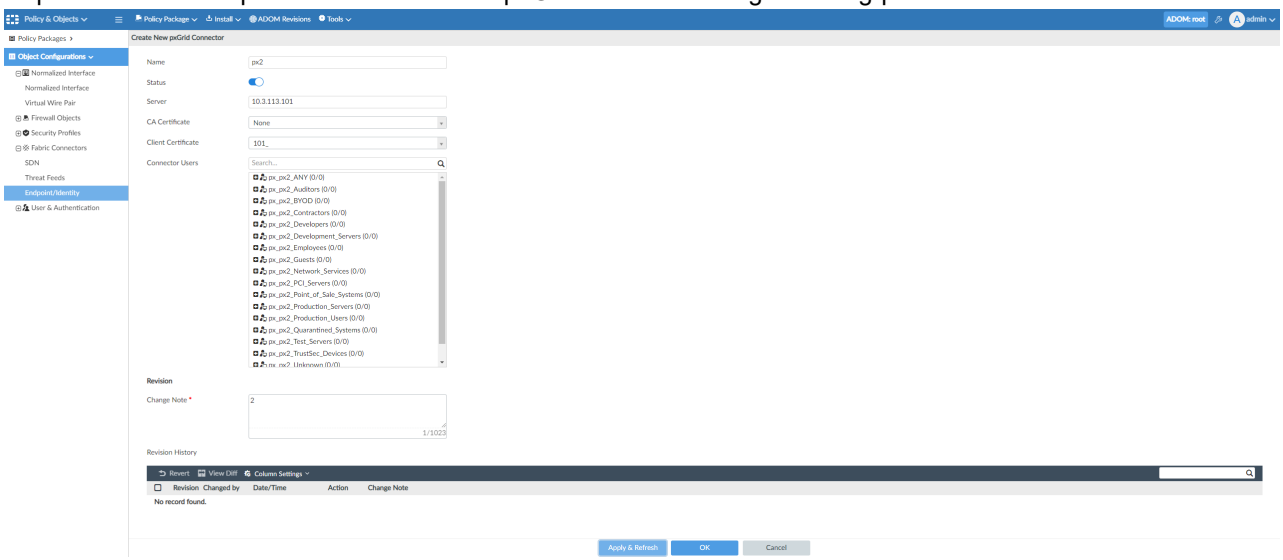
FortiManager allows multiple Cisco PxGrid connectors to be created in the same ADOM.

**To create multiple pxGrid connectors in one ADOM:**

1. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *Endpoint/Identity*.
2. Click *Create New*, and select *pxGrid Connector* from the dropdown menu.
3. Create the first pxGrid connector and get the adgrps from the server.



4. Repeat the above steps and create a second pxGrid connector and get the adgrps from the server.




# FortiManager updated integration with NSX-T

FortiManager has updated integration with NSX-T. Using the new Service Manager APIs, FortiManager gets notifications for registration changes and dynamic address updates.

**To configure NSX-T integration with FortiManager:**

1. Configure the NSX-T connector on page 203
2. Configure the NSX-T Manager on page 205
3. Use the groups in a FortiManager policy on page 208

## Configure the NSX-T connector

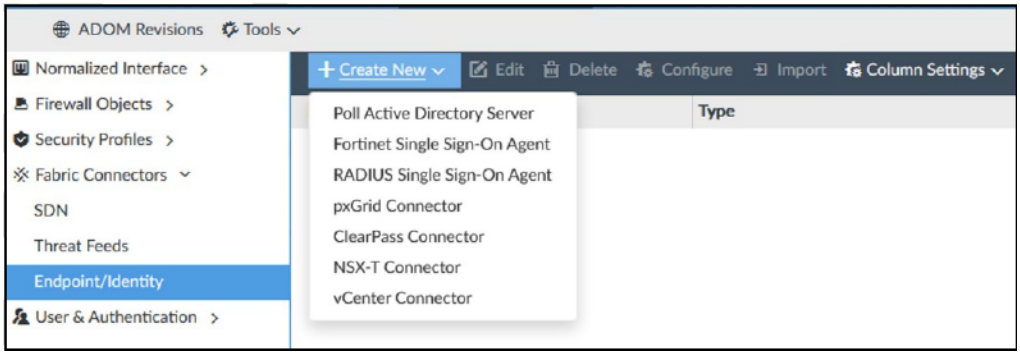
**To enable JSON API access for administrators:**

1. In FortiManager, go to System *Settings* > *Admin* > *Administrators*.
2. Select your Administrator account, and click *Edit*.
3. From the JSON API Access dropdown, select *Read-Write*, and click *OK*.
   The FortiManager will log you out to activate the settings.

**To configure NSX-T API integration on FortiManager:**

1. Log into FortiManager.
2. Go to *Policy & Objects* > *Objects Configuration* > *Fabric Connectors* > *Endpoint/Identity*.

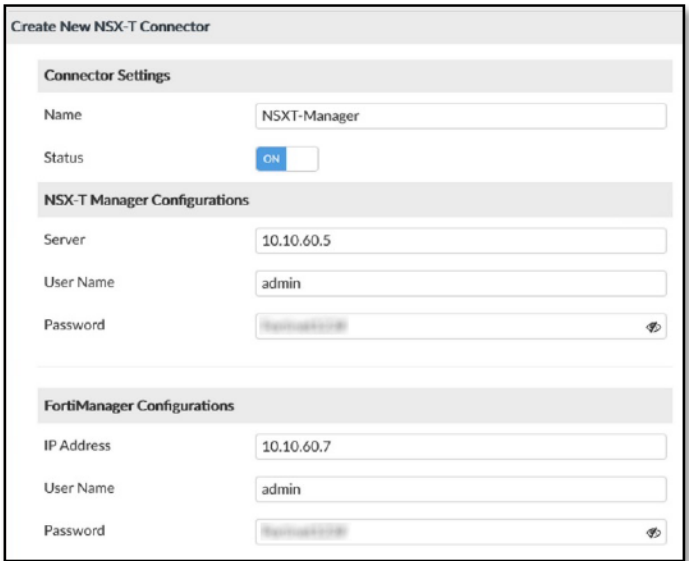
3. Click *Create New* > *NSX-T Connector*.




4. Configure the parameters for the new NSX-T connector, and click *OK*.
   For example:
   a. *Name*: NSXT-Manager.
   b. *Status*: ON.
   c. NSX-T Manager Configurations:
      i. *Server*: NSX-T server.
      ii. *User Name*: NSX-T user name.
      iii. *Password*: NSX-T password.
   d. FortiManager Configurations:
      i. *IP Address*: FortiManager IP or FQDN.
      ii. *User Name*: Your FortiManager administrator user name.

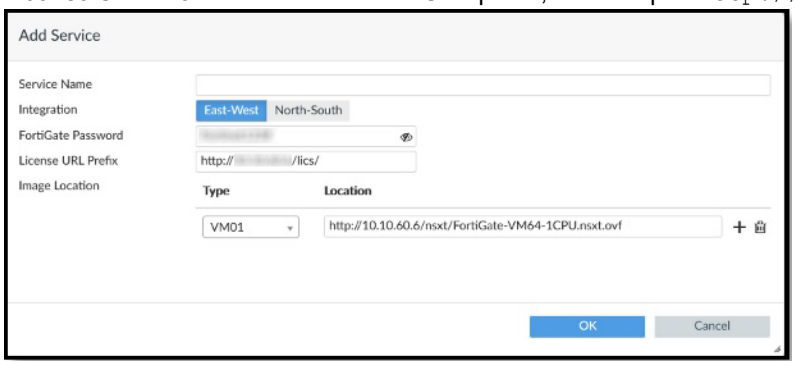
The user name under FortiManager configurations can be any other FortiManager local user with JSON API access set to read-write. This user will be used by the NSX-T Manager to perform the API calls to the FortiManager in order to dynamically update the VM groups objects.

      iii. Password: Your administrator password.

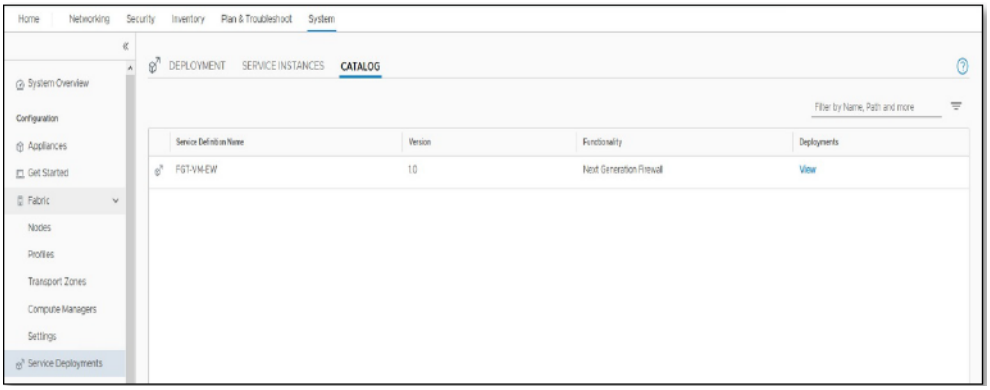



5. Edit the configured NSX-T connector, and click *Add Service* under *Registered Services*.

6. Configure the service details:
   a. *Integration*: Select your integration, for example *East-West*.
   b. *FortiGate Password*: Your FortiGate admin password.
   c. *License URL Prefix*: Enter the license URL prefix, for example: `http://x.x.x.x/lics/`.




7. Click the plus icon to add a new image location, and click *OK*.
   a. *Type*: Select the VM type, for example VM01.
   b. *Location*: Enter the image location, for example: `http://x.x.x.x/FortiGate-VM64xCPU.nsxt.ovf`.
8. In the NSX-T Manager GUI, go to *System* > *Service Deployment* > *CATALOG* to confirm that the FortiGate-VM service was properly registered on NSX-T Manager.

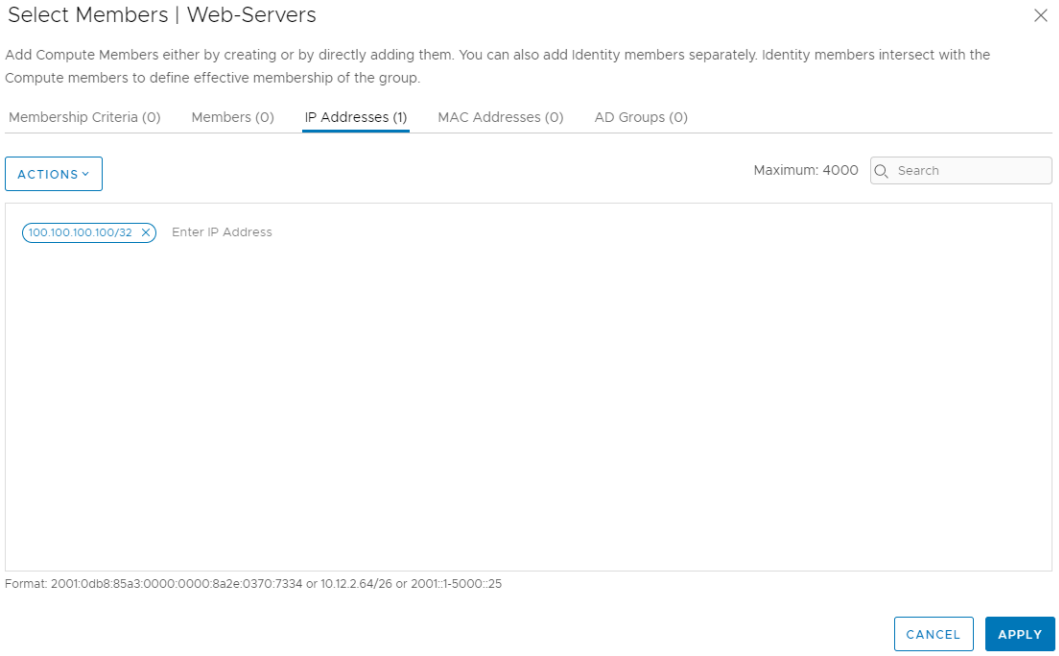



## Configure the NSX-T Manager

**To configure NSX-T Manager:**

1. In the NSX-T Manager GUI, go to *Inventory* > *Groups*, and click *ADD GROUP*.
2. Enter a name, and click *Set Members*.

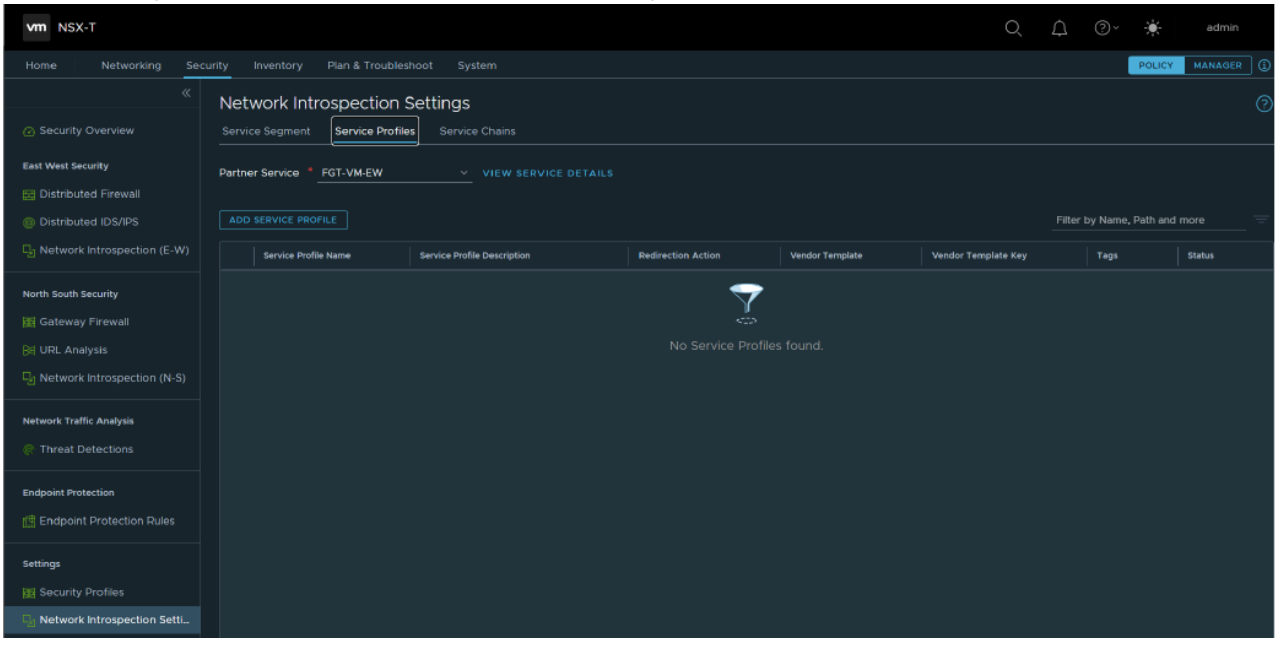
3. Select the *IP Addresses* tab, and add the IP addresses to add as members of this group.



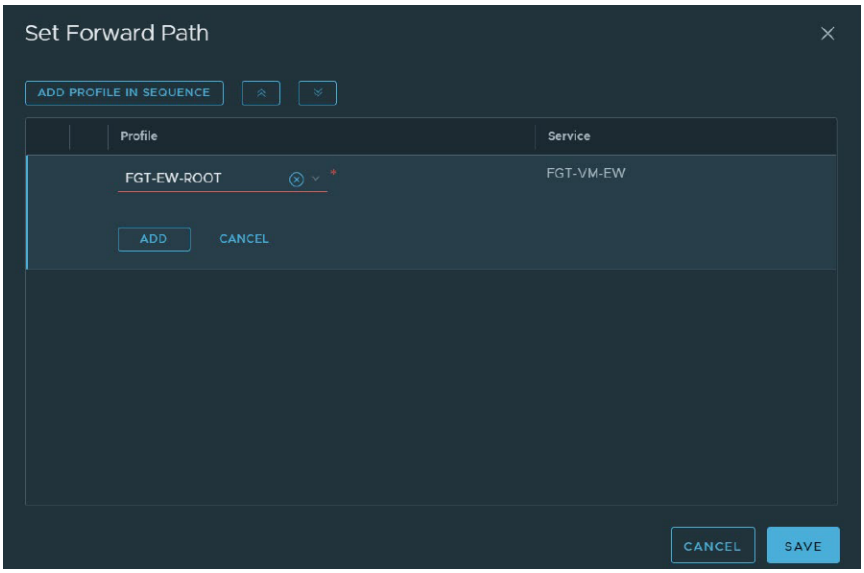

4. Save your changes, and repeat these steps until you have created all of the groups that you require.

Group membership is what is used to determine dynamic NSX-T addresses in FortiManager. There are multiple criteria which can be defined on the NSX-T Manager to make a virtual machine part of that group.

5. Go to *Security* > *Network Introspection Settings* > *Service Profiles*.
6. Select the *Registered Service* from the *Partner Service* dropdown list, and click *ADD SERVICE PROFILE*.



7. Configure the following parameters, and click *Save*.
   a. *Name*: Enter a name.
   b. *Vendor Template*: Select the template listed in the dropdown.
8. Go to the *Service Chains* tab and click *ADD CHAIN*.
9. Configure the following parameters, and click *Save*.
   a. *Name*:Enter a name.
   b. *Service Segment*: Service-Segment.
10. Click *Set Forward Path*, and then click *ADD PROFILE IN SEQUENCE*.




11. Select the profile you just created, and click *ADD*.
12. Save your changes.
13. Go to *East West Security* > *Network Introspection (E-W)*, and click on *Add Policy*.
14. Click on the policy name and you can change it if required.

**To create the redirection rule in NSX-T:**

1. Select the policy you created in the previous step, and click *ADD RULE*.
2. Configure the parameters as follows:
   a. *Name*: Redir-Rule.
   b. *Source*: Any (Groups needs to be selected).
   c. *Destination*: Any (Groups needs to be selected).
   d. *Services*: Any.
   e. *Applied To*: DFW.
   f. *Action*: Redirect.

   This rule will redirect all traffic to the FGT-EW-VM instance. You can be more granular by selecting any combination of *Sources*, *Destinations*, *Services*, or *Applied To* for specific groups. If specific groups are selected, only they will be associated with the Service Manager and show up on FortiManager.
3. Click *PUBLISH* to apply the changes.

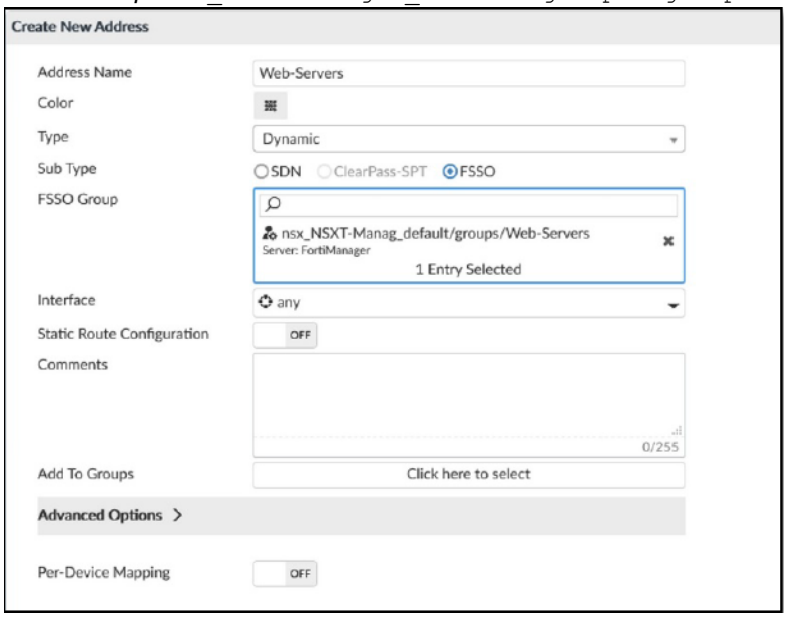
### Use the groups in a FortiManager policy

**To use groups in a policy:**

1. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors*.
2. Edit the NSXT-Manager object.
3. Scroll down and check that the objects with addresses appear. If there aren't any objects, select *Apply & Refresh*.
4. Click *Cancel*.

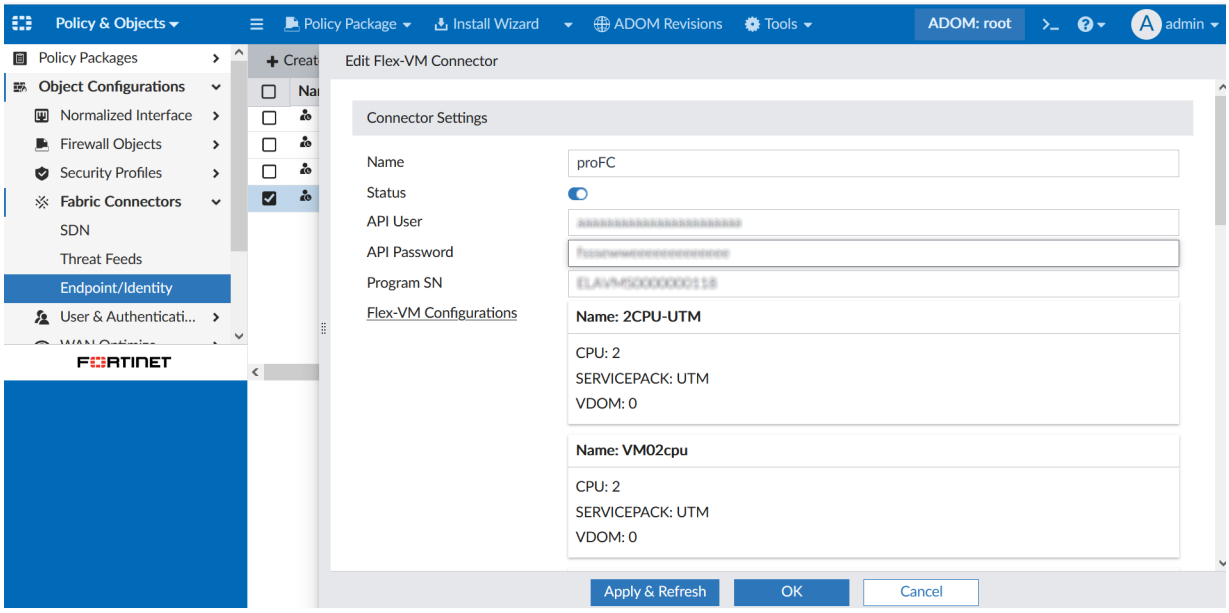
These groups and their members are automatically synchronized between FortiManager and NSX-T Manager. As soon as you add a VM/IP to a group that the Redir-Rule applies to on NSX-T Manager, it will be synchronized.

5. You can have the FortiManager create Firewall Addresses or create your own. Go to *Firewall Objects* > *Addresses*, and click *Create New* > *Address*.
6. Configure the parameters, and click *OK*.
   a. *Address Name*: Enter a name.
   b. *Type*: Dynamic.
   c. *Sub Type*: FSSO.
   d. *FSSO Group*: `nsx_NSXT-Manager_Default/groups/<group name>`

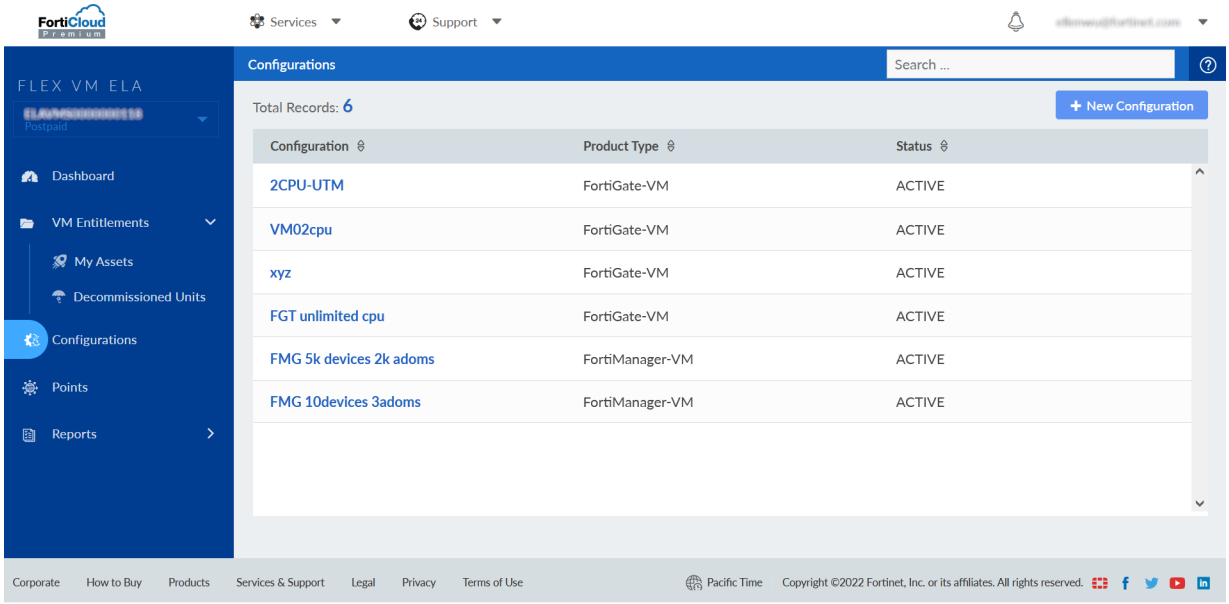



## Flex-VM Fabric Connector to support flex licensing management from FortiManager - 7.2.1

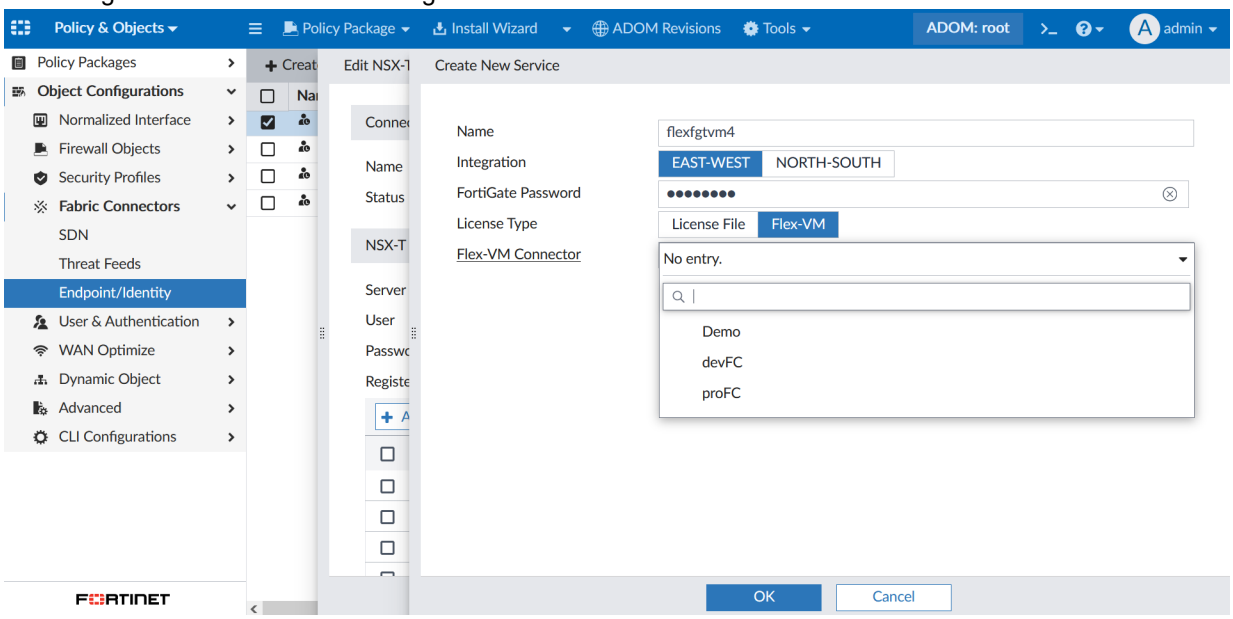
- Flex-VM fabric connectors have been added to FortiManager which can connect to the FortiCare Flex-VM program to retrieve FortiGate Flex-VM configurations.

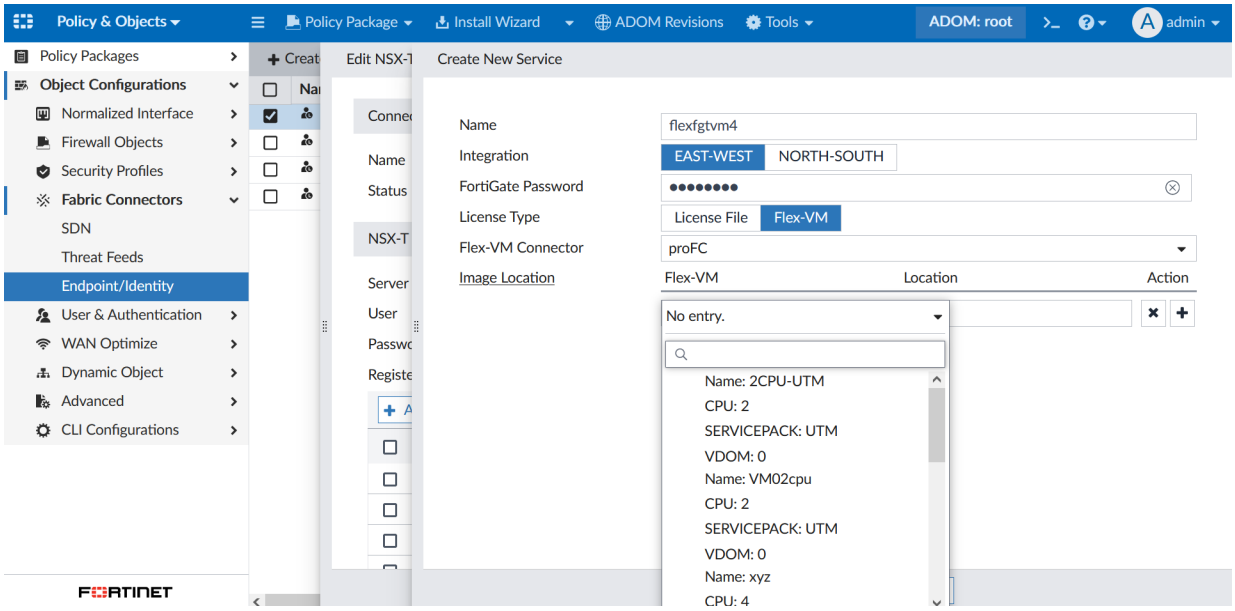



- In Flex-VM, you can view FortiGate Flex-VM configuration details.



- NSX-T FortiGate deployment license types have added the Flex-VM license option which can fetch FortiGate Flex-VM configurations from the FortiManager Flex-VM connector.



# System

This section lists the new features added to FortiManager for system settings:



# High Availability (HA)

This section lists the new features added to FortiManager for high availability (HA):

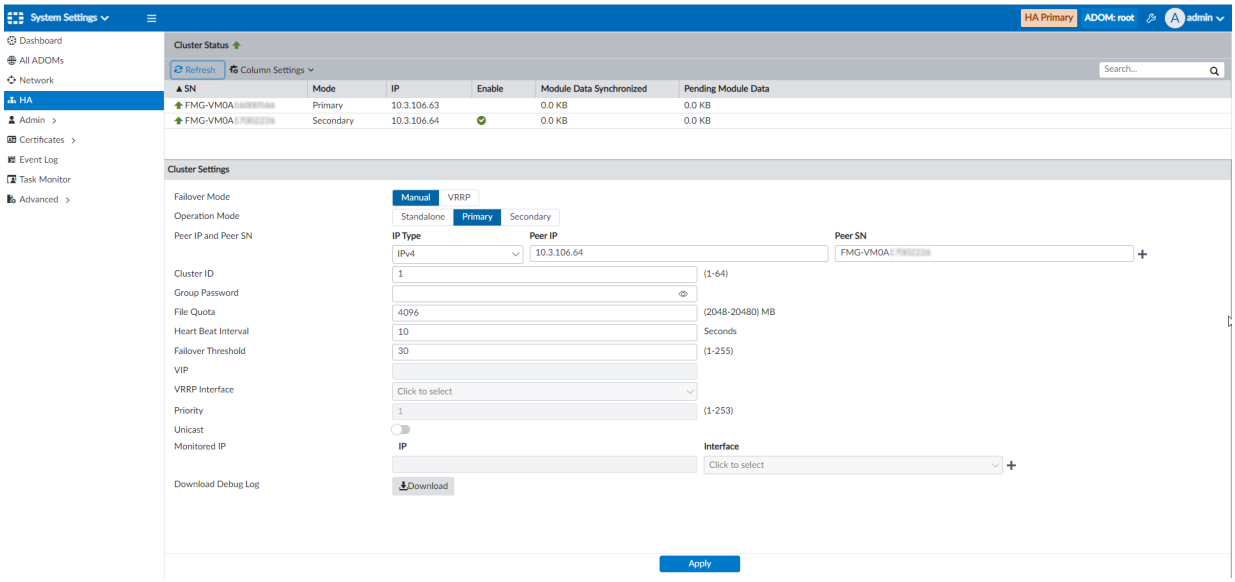


## FortiManager-HA automatic failover enhancement

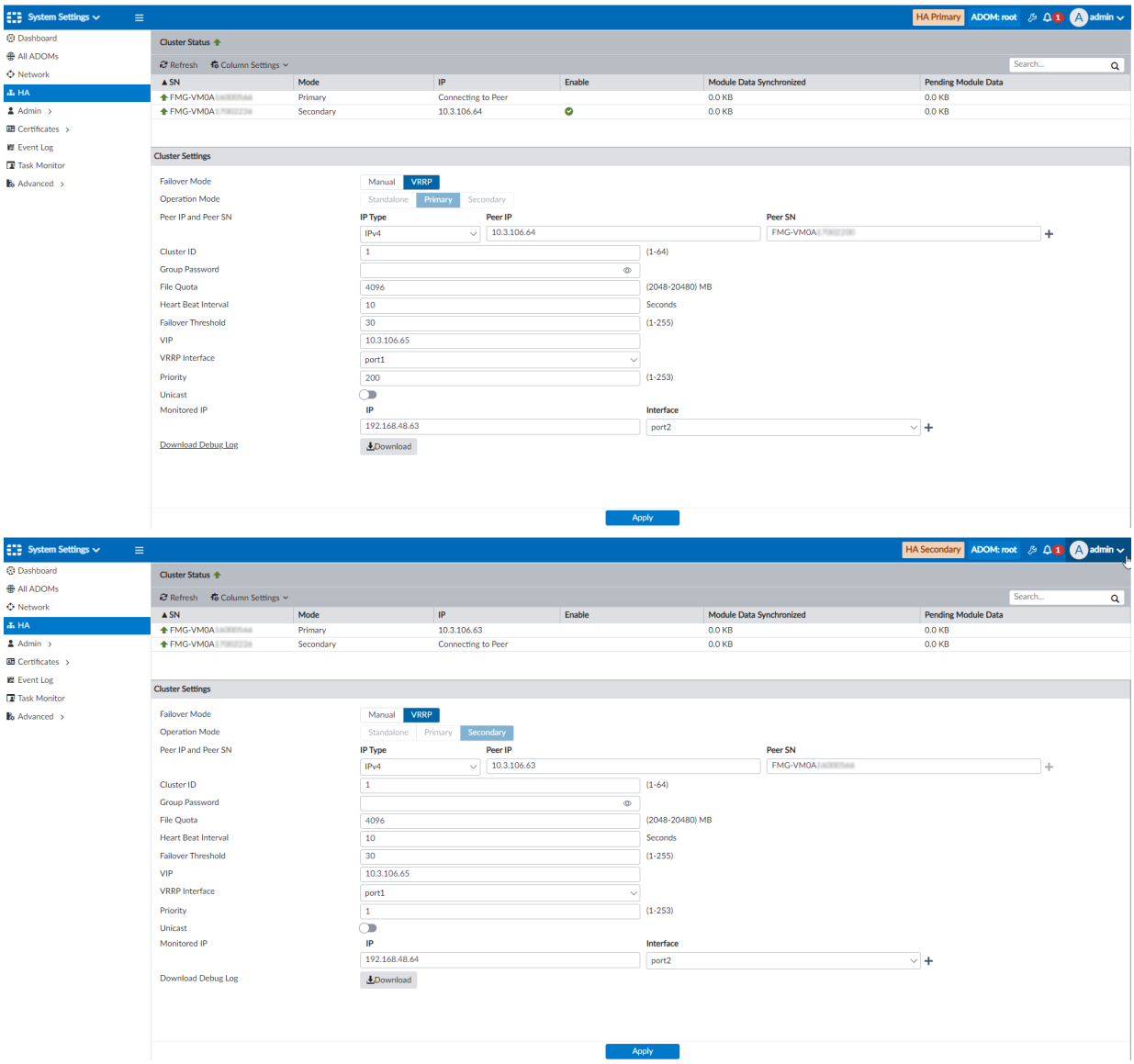
This feature introduces automatic failover for FortiManager-HA.

**To use automatic failover for FortiManager-HA:**

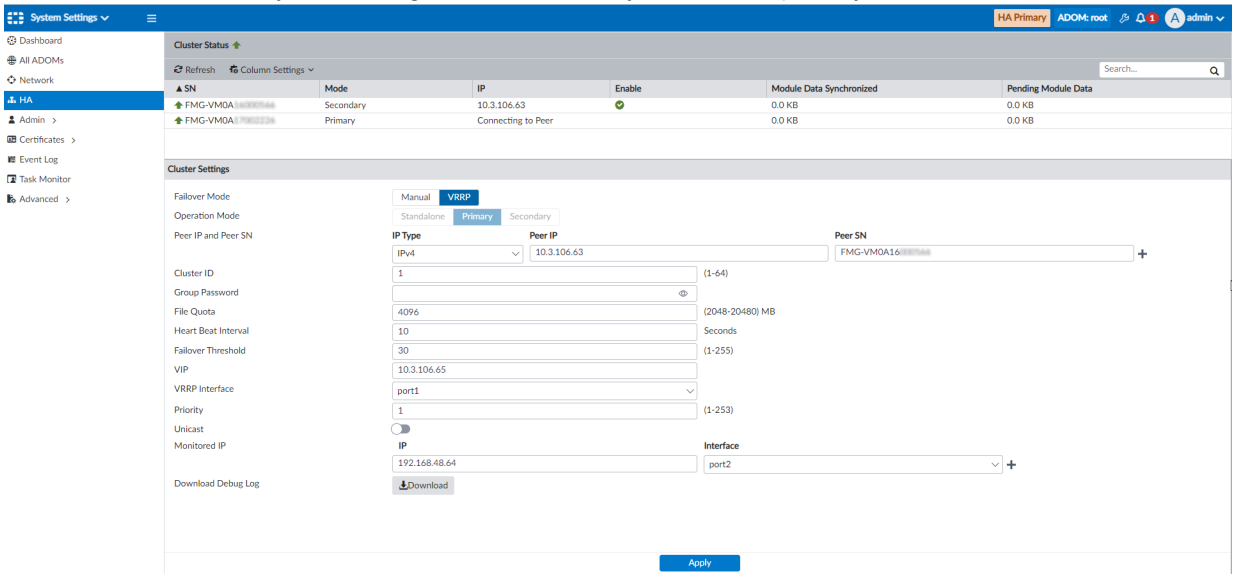
1. In FortiManager, go to *System Settings* > *HA*.
   A new *Failover Mode* setting is available in the FortiManager HA configuration menu. You can select *Manual* for manual failover or *VRRP* to enable automatic failover.




2. Select *VRRP* as the *Failover Mode*, and configure the other settings required including the *VIP*, *VRRP Interface*, *Priority*, *Unicast*, and *Monitored IP*.


System Settings
HA Primary
ADOM: root
admin
Dashboard
All ADOMs
Network
HA
Admin
Certificates
Event Log
Task Monitor
Advanced
Cluster Status
Refresh
Column Settings
Search...
SN
Mode
IP
Enable
Module Data Synchronized
Pending Module Data
FMG-VM0A
Primary
Connecting to Peer
0.0 KB
Secondary
10.3.106.64
Cluster Settings
Failover Mode
Manual
VRRP
Operation Mode
Standalone
Primary
Secondary
Peer IP and Peer SN
IP Type
Peer IP
Peer SN
IPv4
Cluster ID
(1-64)
Group Password
File Quota
4096
(2048-20480) MB
Heart Beat Interval
10
Seconds
Failover Threshold
30
(1-255)
VIP
10.3.106.65
VRRP Interface
port1
Priority
200
Unicast
Monitored IP
IP
Interface
192.168.48.63
port2
Download Debug Log
Download
Apply
System Settings
HA Secondary
ADOM: root
admin
Dashboard
All ADOMs
Network
HA
Admin
Certificates
Event Log
Task Monitor
Advanced
Cluster Status
Refresh
Column Settings
Search...
SN
Mode
IP
Enable
Module Data Synchronized
Pending Module Data
FMG-VM0A
Primary
10.3.106.63
0.0 KB
Secondary
Connecting to Peer
Cluster Settings
Failover Mode
Manual
VRRP
Operation Mode
Standalone
Primary
Secondary
Peer IP and Peer SN
IP Type
Peer IP
Peer SN
IPv4
Cluster ID
(1-64)
Group Password
File Quota
4096
(2048-20480) MB
Heart Beat Interval
10
Seconds
Failover Threshold
30
(1-255)
VIP
10.3.106.65
VRRP Interface
port1
Priority
1
(1-253)
Unicast
Monitored IP
IP
Interface
192.168.48.64
port2
Download Debug Log
Download
Apply

3. When the monitored interface for the Primary FortiManager is unreachable or down, HA automatic failover will occur, and the Secondary FortiManager will automatically become the primary.




### To configure automatic failover in the FortiManager CLI:

1. On the Primary FortiManager, configure the FortiManager settings with VRRP mode selected:

```
config system ha
   set failover-mode vrrp
      config monitored-ips
         edit 1
            set interface <string>
            set ip <string>
         next
      end
      config peer
         edit <peer_id_int>
            set ip <peer_ipv4_address>
            set serial-number <string>
         next
      end
   set priority <integer>
   set vip <string>
   set vrrp-interface <string>
end
```

For example:

```
config system ha
   set failover-mode vrrp
      config monitored-ips
         edit 1
            set interface "port2"
            set ip "192.168.48.63"
         next
      end
      config peer
         edit 1
            set ip 10.3.106.64
            set serial-number "FMG-VM0A17001234"
```

```
        next
      end
   set priority 200
   set vip "10.3.106.65"
   set vrrp-interface "port1"
end
```

2. On the Secondary FortiManager, configure the FortiManager settings with VRRP mode selected:

```
config system ha
   set failover-mode vrrp
      config monitored-ips
         edit <id>
            set interface <string>
            set ip <string>
         next
      end
config peer
   edit <peer_id_int>
      set ip <peer_ipv4_address>
      set serial-number <string>
   next
end
   set vip <string>
   set vrrp-interface <string>
end
```

For example:

```
config system ha
   set failover-mode vrrp
      config monitored-ips
         edit 1
            set interface "port2"
            set ip "192.168.48.64"
         next
      end
config peer
   edit 1
      set ip 10.3.106.63
      set serial-number "FMG-VM0A16001234"
   next
end
   set vip "10.3.106.65"
   set vrrp-interface "port1"
end
```

# Administrators

This section lists the new features added to FortiManager for administrators:

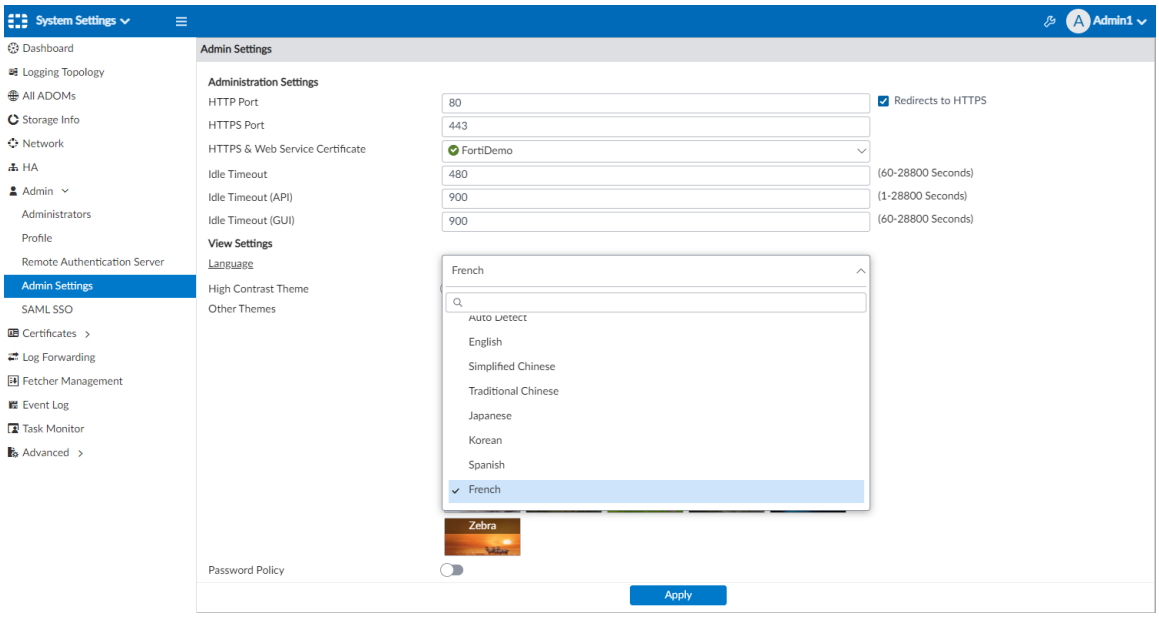
## Add French language support to GUI

FortiManager GUI now supports French in addition to the previously supported languages.

By default, the GUI language is set to *Auto Detect*, which automatically uses the language set for the administrator's browser. If that language is not supported, the GUI defaults to English.

**To set the GUI language to French:**

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. From the *Language* dropdown, select *French*.
3. Click *Apply*.

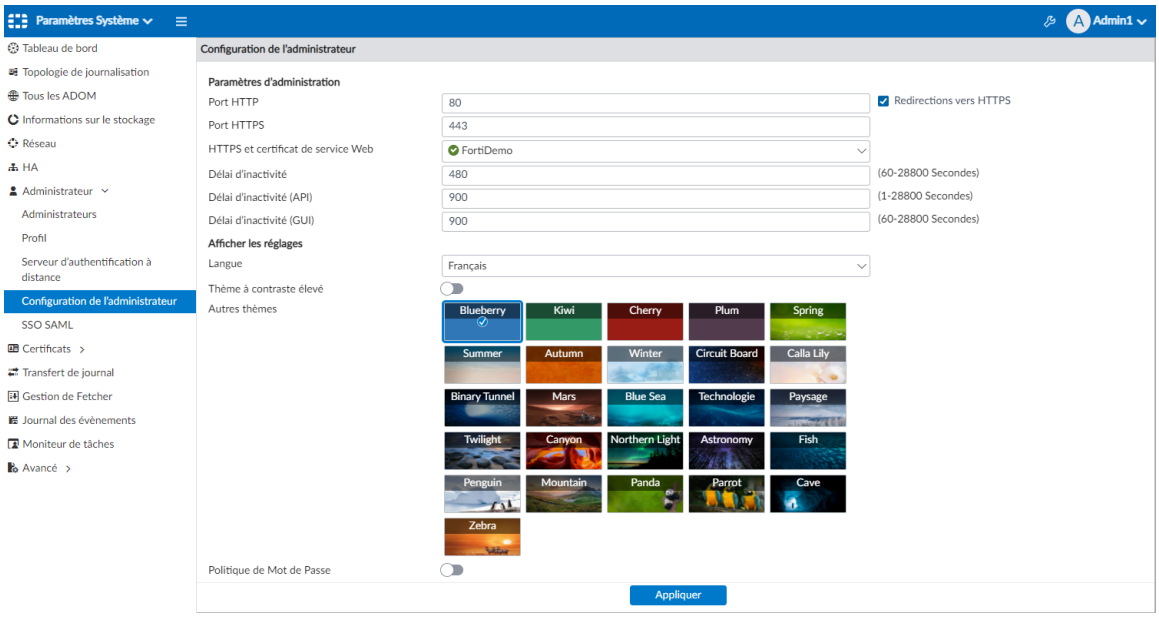



**To set the GUI language to French from the CLI:**

```
config system admin setting
   set webadmin_language french
end
```

This setting does not affect the CLI.

Below is an example of the French GUI:




## New firewall admin role with no RW permission on IPS objects

From the CLI, you can set none, read-only, and read-write permissions on IPS objects for an admin profile. Previously, you could not set read-only permissions on IPS objects.

**To set permissions on IPS objects:**

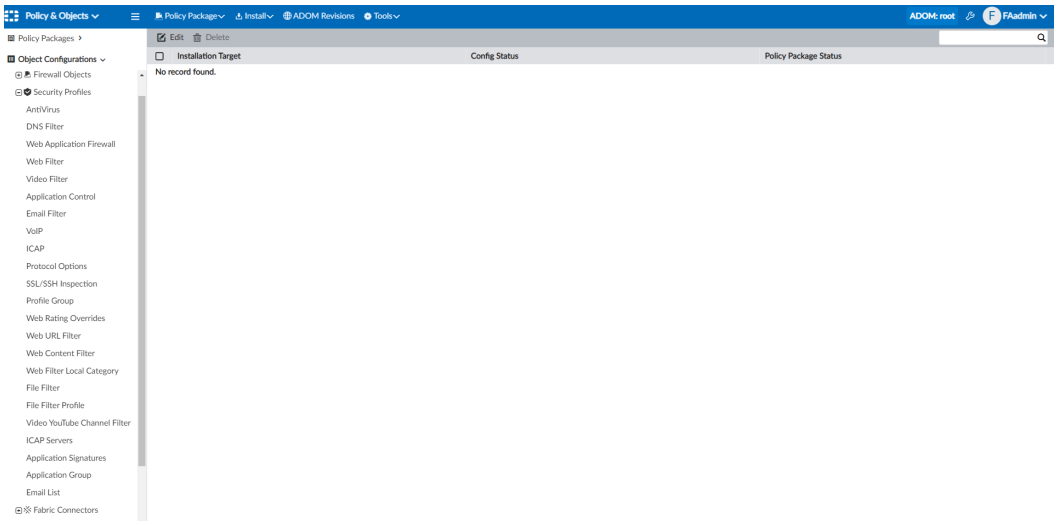
1. In the FortiManager CLI, enter the following command:

```
config system admin profile
   edit <profile>
      set ips-objects {none | read | read-write}
   next
end
```

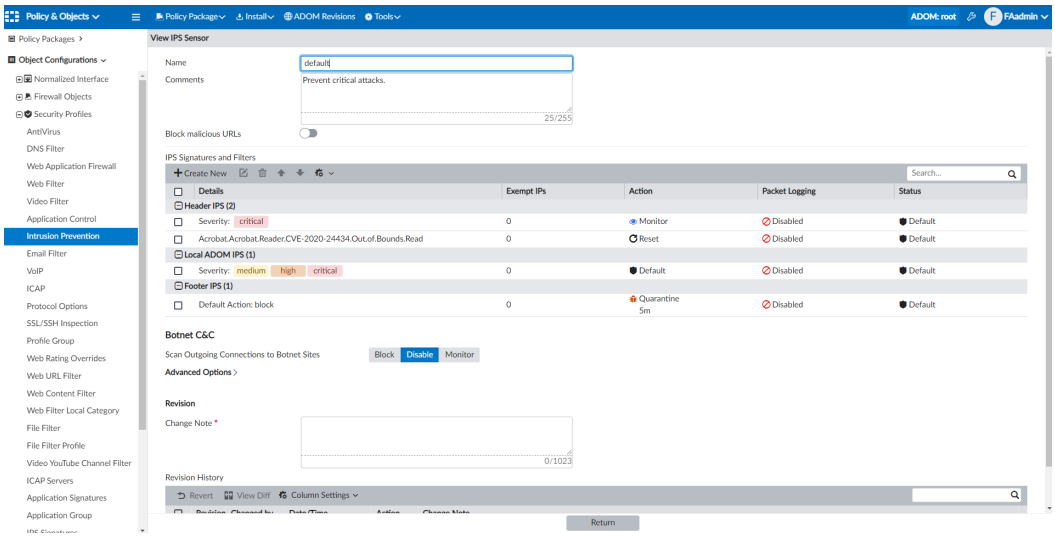
You cannot edit this profile setting from the GUI. It must be done in the CLI.

2. In the FortiManager GUI or CLI, assign this profile to administrators, as needed.

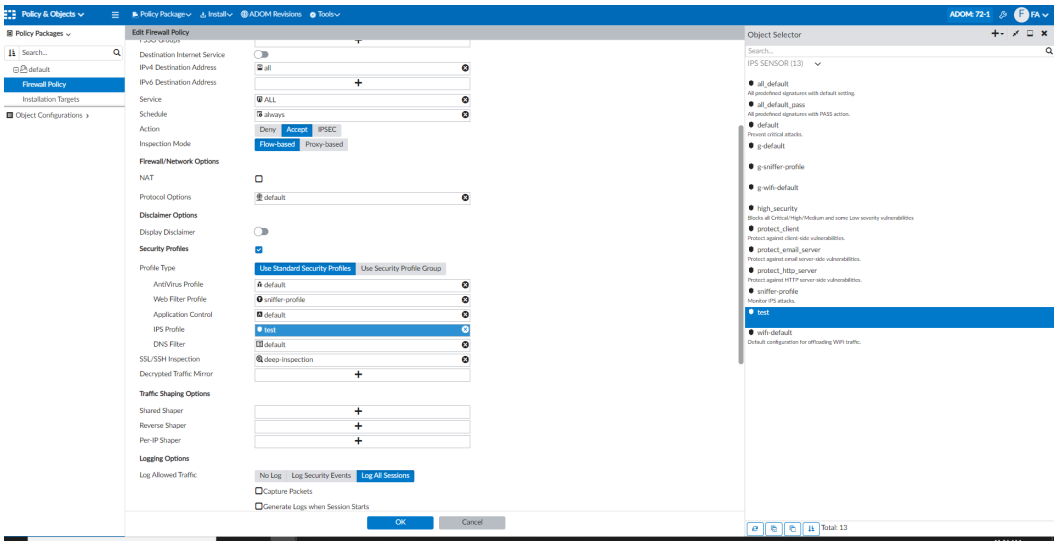
- If `ips-objects` is set to `none`, administrators with this profile cannot see IPS objects.




- If `ips-objects` is set to `read`, administrators with this profile can read but not edit or install IPS objects.




- Administrators with `ips-objects` read-only permissions can install firewall policies without installing IPS related objects. They can also assign IPS profiles in the policy package.



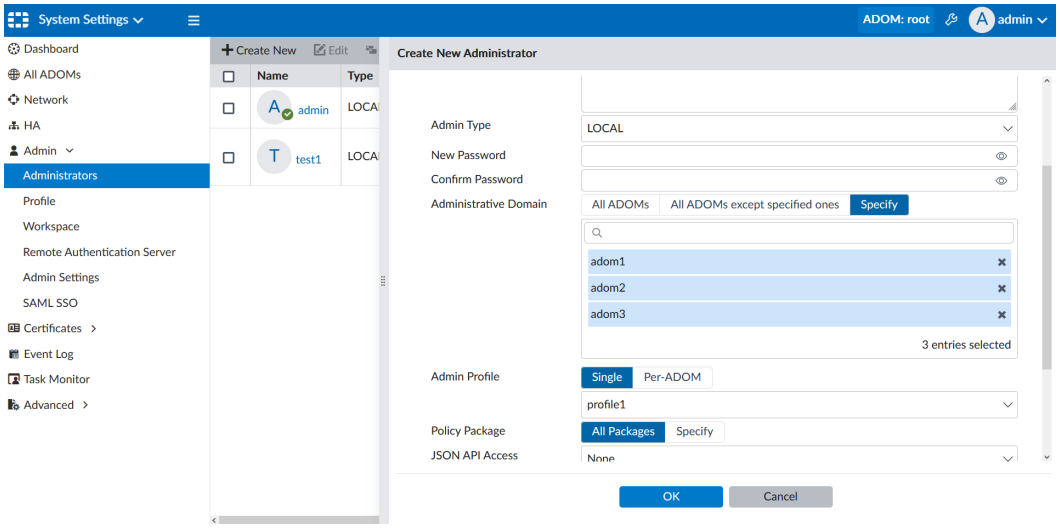
- If `ips-objects` is set to `read-write`, administrators with this profile can edit and install IPS objects in addition to the `ips-objects` read-only privileges.

## Per-ADOM admin profile - 7.2.1

A per-ADOM admin profile allows the administrator to log in on different ADOMs with different admin profiles.

**To assign a per-ADOM admin profile:**

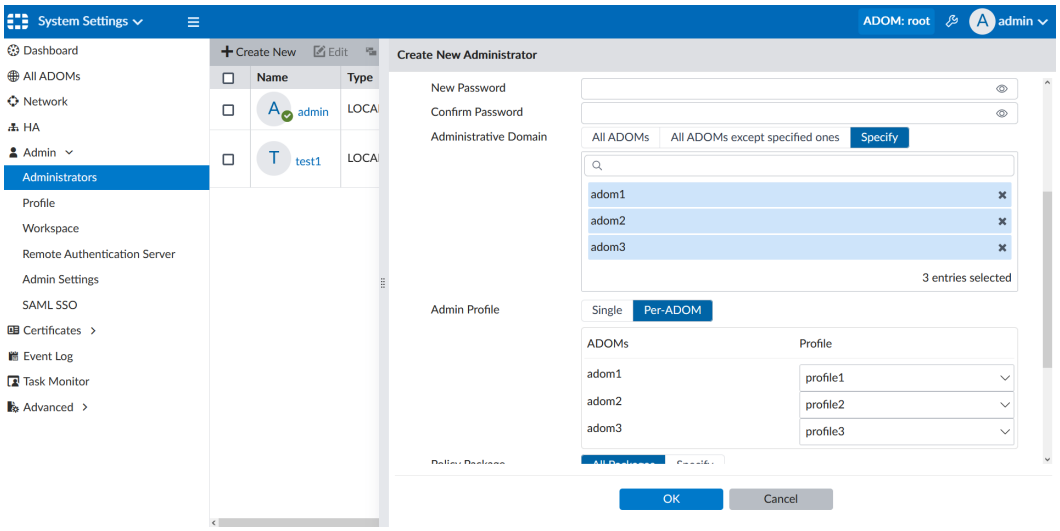
1. Go to *System Settings* > *Admin* > *Administrators*, and click *Create New*.
   Alternatively, you can select an existing administrator and click *Edit*.
2. For *Administrative Domain*, select *Specify*.
3. For *Administrative Domain*, click *Click to select* to open the list of available ADOMs.
4. Select the ADOMs the administrator will be able to access, and click *OK*.



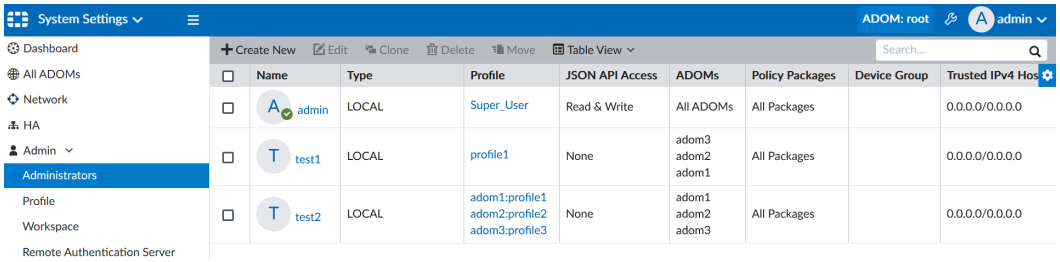

5. For *Admin Profile*, select *Per-ADOM*.
   If *Single* is selected, the administrator will only have one admin profile for all ADOMs.

When *Per-ADOM* is selected, the *Admin Profile* setting displays the list of ADOMs that you specified access to for the administrator. A *Profile* dropdown is available for each ADOM.

6. Using the *Profile* dropdowns, select an admin profile for each ADOM.
   The profile determines the administrator's access to the FortiManager features when they are in that ADOM.
   In the example below, a different profile is selected for each ADOM. The administrator will have profile1 access in adom1, profile2 access in adom2, and profile3 access in adom3.




7. Configure the other settings for the administrator, and click *OK*.
   In *System Settings* > *Admin* > *Administrators*, the *Profile* column lists the profiles selected per-ADOM. For example, see *test2* in the image below.




# Network

This section lists the new features added to FortiManager for networks:

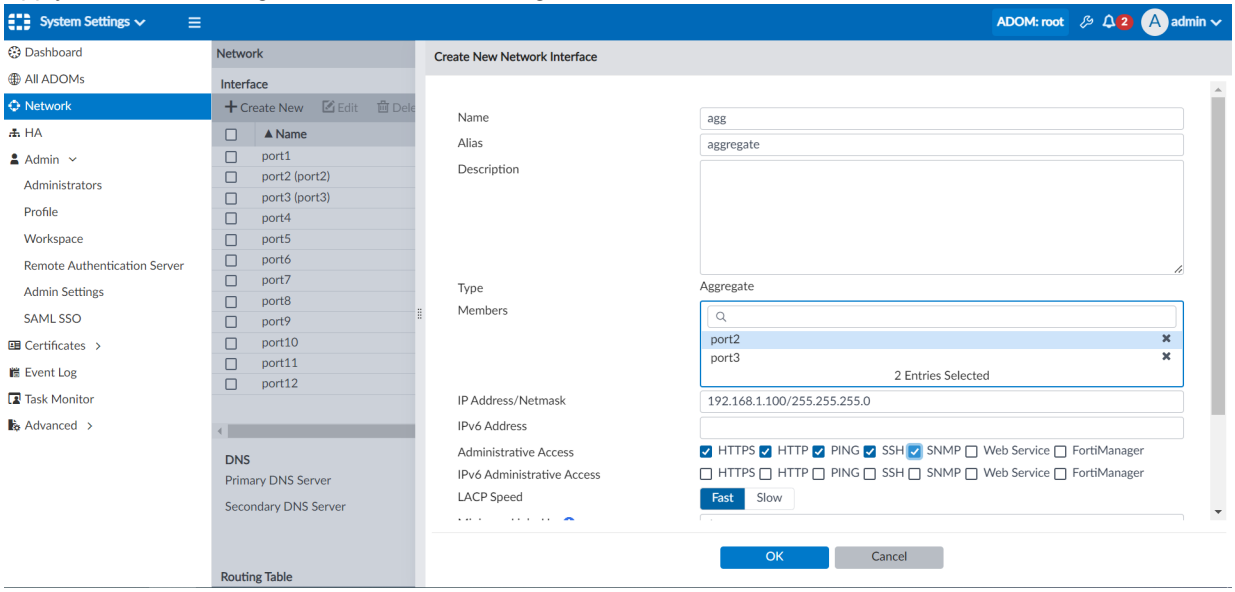

- FortiManager supports link aggregation of physical ports on page 219
- FortiManager supports VLANs on physical network interfaces on page 221


## FortiManager supports link aggregation of physical ports

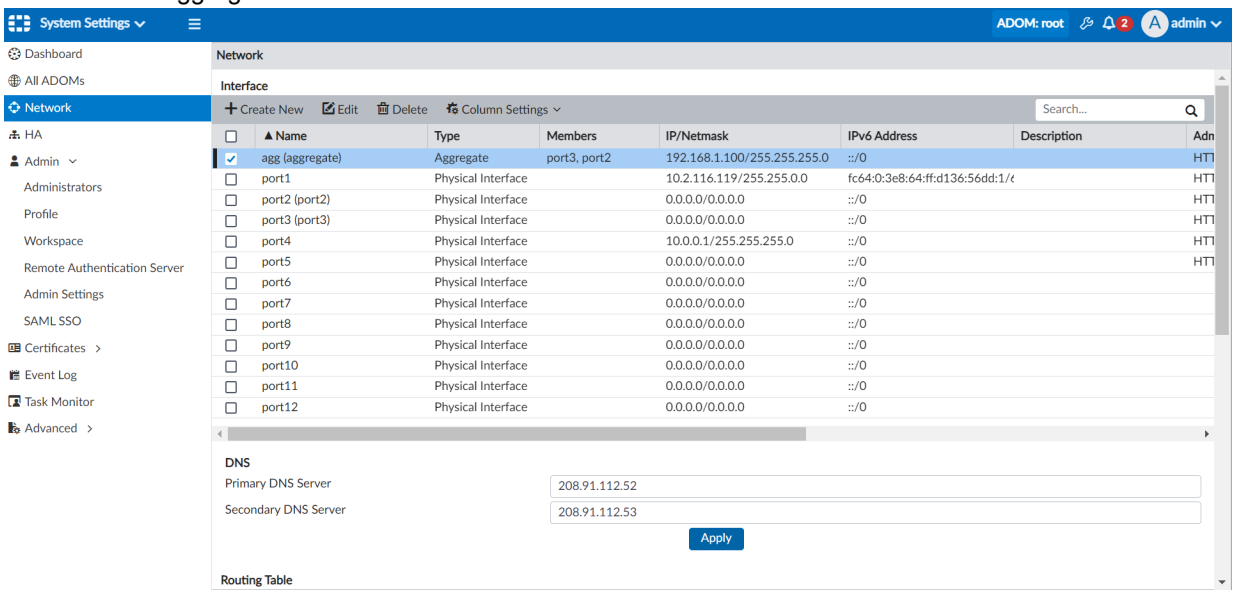
Interface link-aggregation is now supported on FortiManager for physical ports to provide interface redundancy and load balance.

**To create an aggregate interface in the GUI:**

1. Go to *System Settings* > *Network*.
2. In the toolbar, click *Create New*. The *Create New Interface* window opens.
3. In the *Name* field, enter a name for the interface (for example, `Agg`)
4. Click the *Members* field to select the available ports.
5. Apply the default settings for the rest of the configurations.

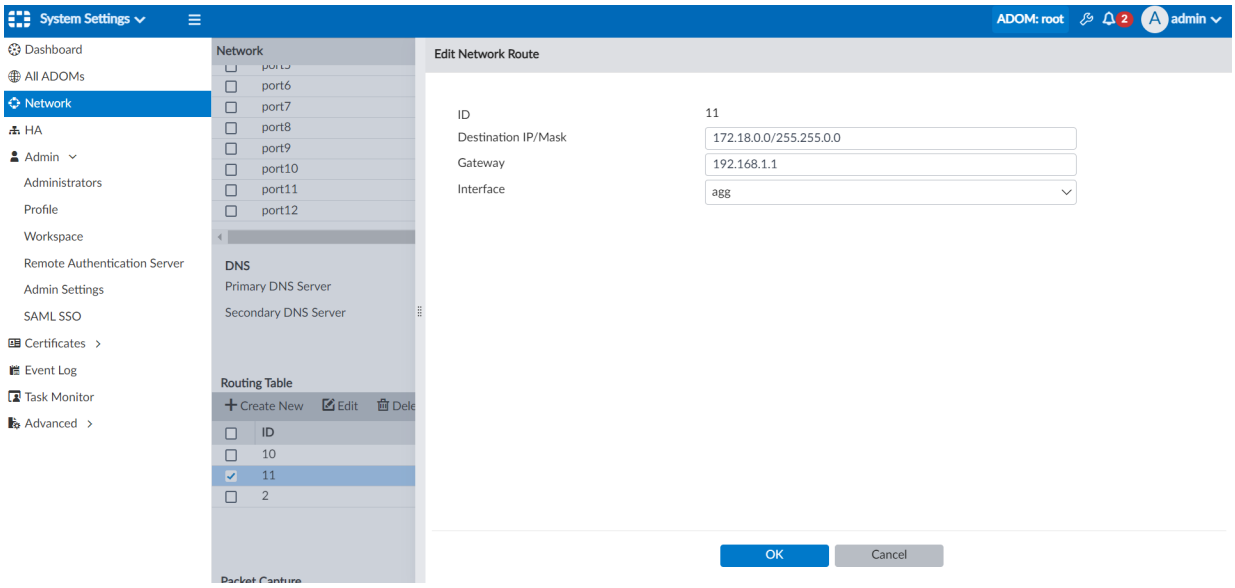



6. Click *OK*. The aggregation interface is created.




7. Configure the static route via the aggregate link. When the aggregate link is configured on the other side, the

connection is complete.



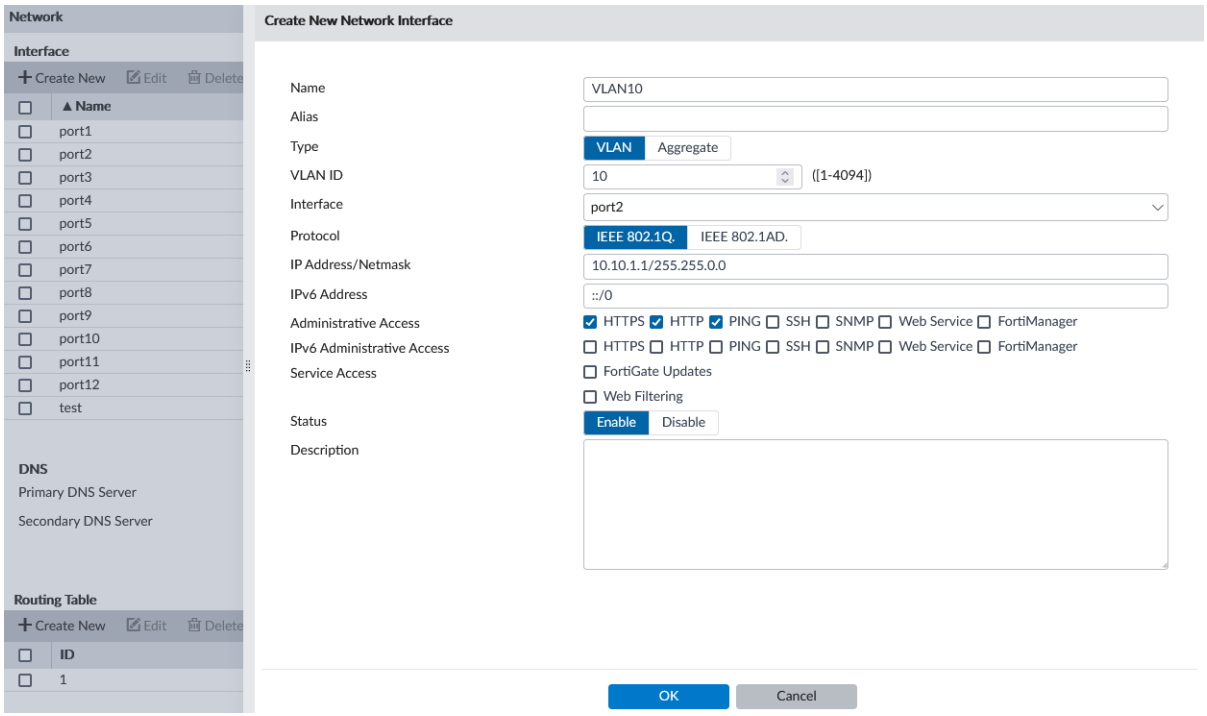

## FortiManager supports VLANs on physical network interfaces

FortiManager supports VLANs on physical network interfaces.

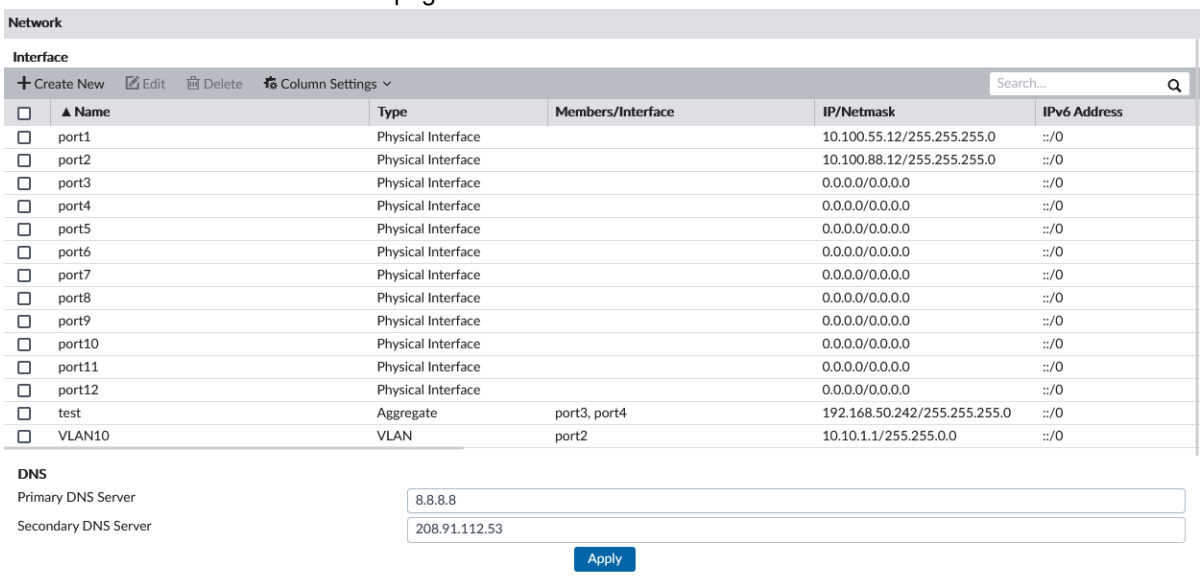
**To create a VLAN on FortiManager:**

1. Go to *System Settings* > *Network*, and click *Create New* in the *Interface* table toolbar. The Create New Network Interface window opens.

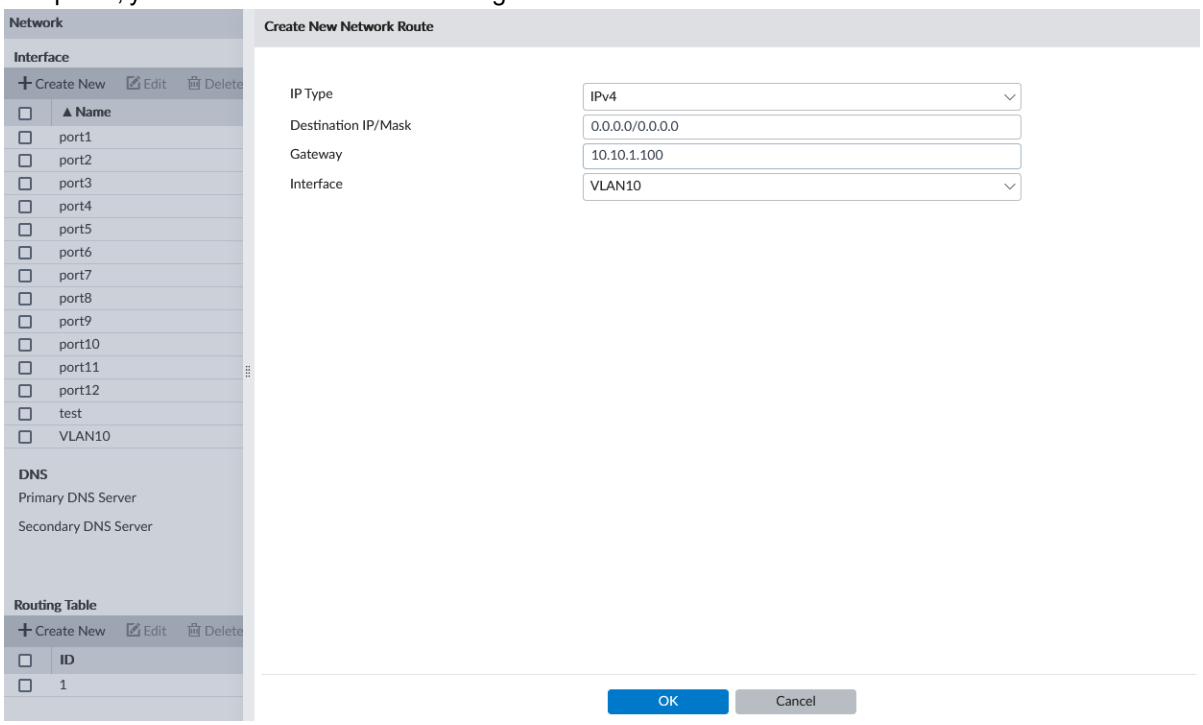
2. Select VLAN as the interface type, and enter the VLAN name, VLAN ID, and the interface to which the VLAN is bound.




3. Click *OK* to save the VLAN.
The VLAN is visible on the network page.



If required, you can create a static route using the VLAN interface.




**To configure VLAN interfaces in the CLI:**

1. Open the FortiManager CLI.
2. Enter the following commands.

```
config system interface
   edit <vlan-name>
      set type vlan
      set interface "portx"
      set vlanid <1-4094>
      set vlan-protocol <8021q/8021ad>
end
```

For example:

```
config system interface
   edit "vlan2"
      set ip 2.2.2.2 255.255.255.0
      set allowaccess ping https ssh
      set type vlan
      set interface "port2"
      set vlanid 2
      set vlan-protocol 8021q
end
```

# Others

This section lists the new features added to FortiManager for other features relating to system settings:

## Add LLDP support on FMG and FAZ - 7.2.1

Using the CLI, the link layer discovery protocol (LLDP) feature can be enabled on FortiManager ports to advertise the device identity and make it discoverable by other devices on the local network segment. After enabling the LLDP feature on a port, the port sends LLDP packets every 30 seconds.

The LLDP feature is set to `disable` by default.

**To enable the LLDP feature:**

1. In the CLI, enter the following command:

```
config system interface
   edit port1
      set lldp enable
   next
end
```

## FortiManager setup wizard improvement with optional firmware upgrade step - 7.2.1

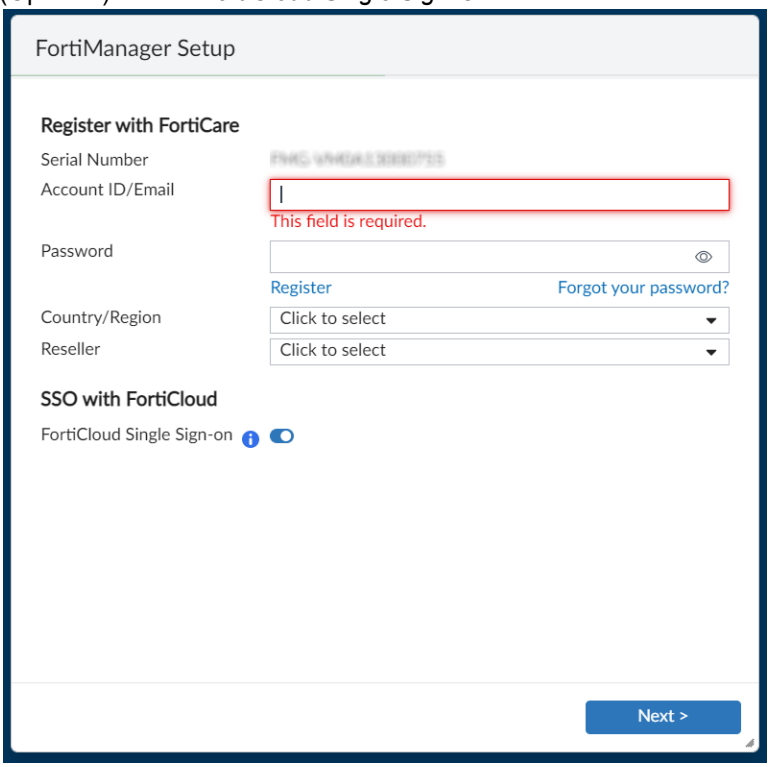
The setup wizard has been enhanced in FortiManager 7.2.1 and now includes the following steps, including optional firmware upgrade step:

1. Register and SSO with FortiCare.
2. Specify Hostname.
3. Change Your Password.
4. Upgrade Firmware.

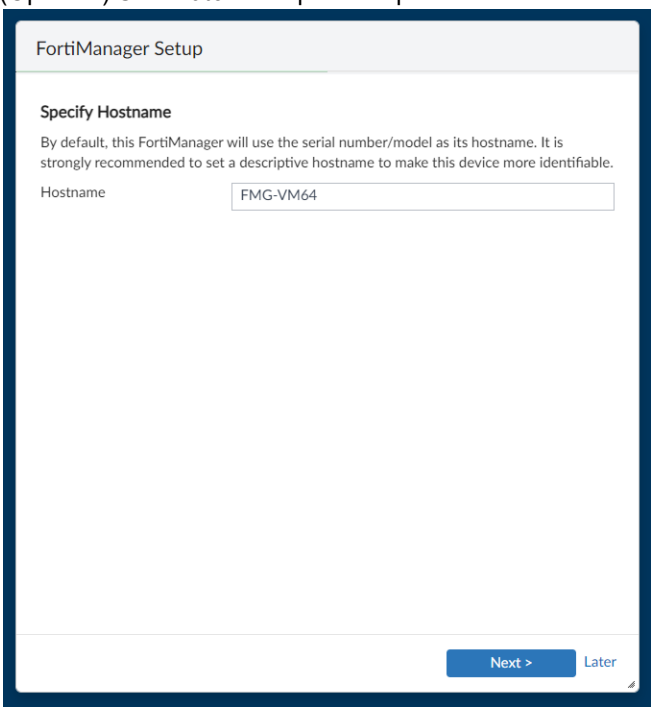
**To setup FortiManager using the wizard:**

1. For an internet connected FortiManager:
   a. Configure the IP address and route to the internet through the FortiManager CLI, and then connect to the FortiManager GUI, and log in with your FortiManager administrator account.
   b. Click *Begin* on the wizard's welcome page.
   c. Enter your FortiCare *Account ID/Email*, *Password*, *Country/Region*, and *Reseller*.

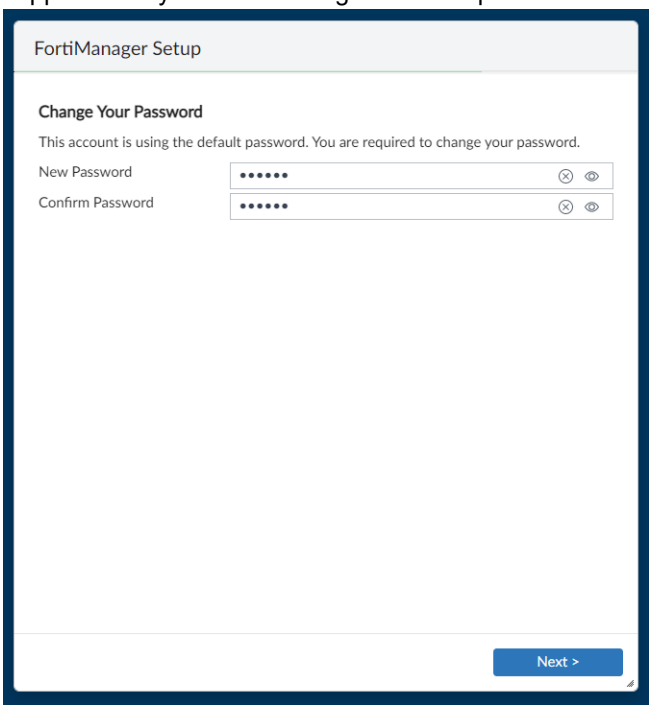
d. (Optional) Enable *FortiCloud Single Sign-On*.



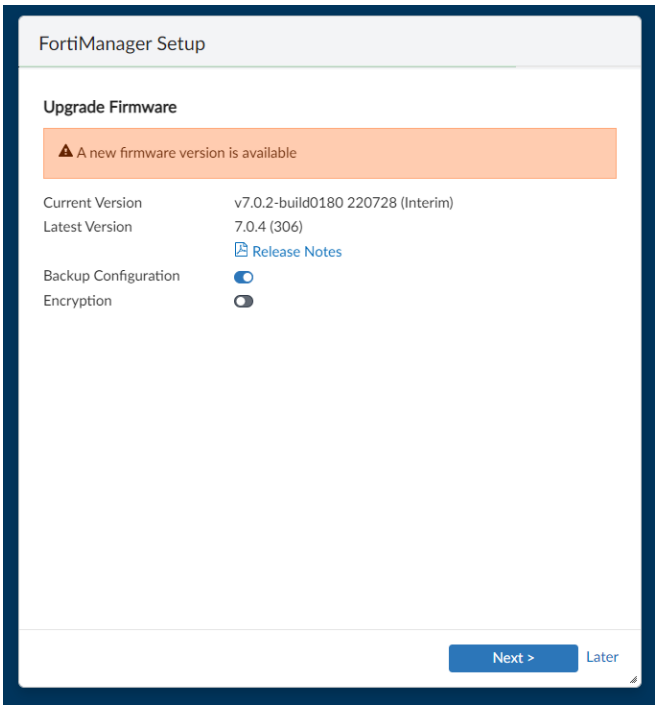

2. After the FortiManager has been registered using one of the methods above, you can specify your hostname in the setup wizard:
   a. Specify the hostname of the FortiManager.
   b. (Optional) Click *Later* to skip this step.

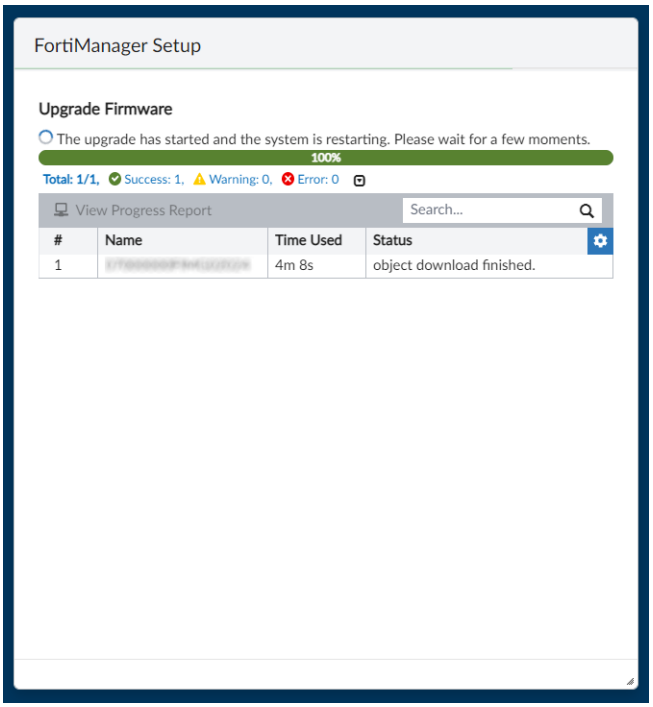


3. Change the default password by entering a new password and confirming the password. This step cannot be skipped when you are still using the default password.




4. Upgrade your firmware to the latest patch for that version. If FortiManager cannot connect to FortiGuard to get the image and upgrade path, then this step will display as passed.
   a. Click *Next* to download the firmware and upgrade to the latest patch.
   b. (Optional) Enable *Backup Configuration* and *Encryption settings*.
   c. (Optional) Click *Later* to skip this step.




5. Once all four steps are passed, the setup wizard page will no longer be displayed.

## TPM hardware module - 7.2.2

An enhanced security layer is added to FortiManager: when private data encryption is enabled, the encryption key is stored securely on the TPM hardware module.

Only select FortiManager hardware models feature a Trusted Platform Module (TPM) that can be used to protect your password and key against malicious software and phishing attacks. This dedicated micro-controller module hardens physical networking appliances by generating, storing, and authenticating cryptographic keys.

For more information about which FortiManager models feature TPM support, see the FortiManager Data Sheet.

The TPM is disabled by default, but it can be enabled from the FortiManager CLI.

To enable TPM, you must enable `private-data-encryption` and set the 32 hexadecimal digit master-encryption-password. This encrypts sensitive data on the FortiManager using AES128-CBC. With the password, TPM generates a 2048-bit primary key to secure the master-encryption-password through RSA-2048 encryption. The master-encryption-password protects the data and the primary key protects the master-encryption-password.

The key is never displayed in the configuration file or the system CLI, thereby obscuring the information and leaving the encrypted information on the TPM.

The primary key binds the encrypted configuration file to a specific FortiManager unit and never leaves the TPM. When backing up the configuration, the TPM uses the key to encrypt the master-encryption-password in the configuration file. When restoring a configuration that includes a TPM protected master-encryption-password:

- If TPM is disabled, then the configuration cannot be restored.
- If TPM is enabled but has a different master-encryption-password than the configuration file, then the configuration cannot be restored.
- If TPM is enabled and the master-encryption-password is the same in the configuration file, then the configuration can be restored.

For more information about backing up the system, restoring the configuration, or migrating the configuration, see the FortiManager Administration Guide.

### To check if your FortiManager device has a TPM:

Enter the following command in the FortiManager CLI:

```
diagnose hardware info
```

The output in the CLI includes `### TPM info`, which displays if the TPM is `detected` (enabled), `not detected` (disabled), or not available.

### To enable TPM and input the master-encryption-password:

Enter the following command in the FortiManager CLI:

```
config system global
   set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
********************************
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
********************************
Your private data encryption key is accepted.
```

# Management Extensions

This section lists the other new features added to FortiManager for management extensions:



## Management Extensions

This section lists the other new features added to FortiManager for management extensions:



## Universal Connector MEA added support for Cisco ACI - 7.2.1

Universal Connector MEA added support for Cisco ACI to retrieve the endpoint groups (EPGs) and operate dynamic objects changes on FortiGates.

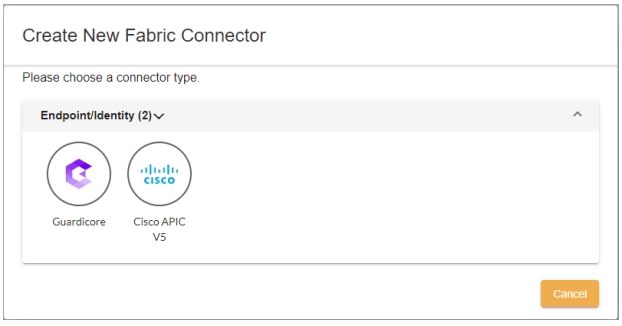
This feature requires Cisco ACI version 5 or higher.



### Creating the Universal Connector

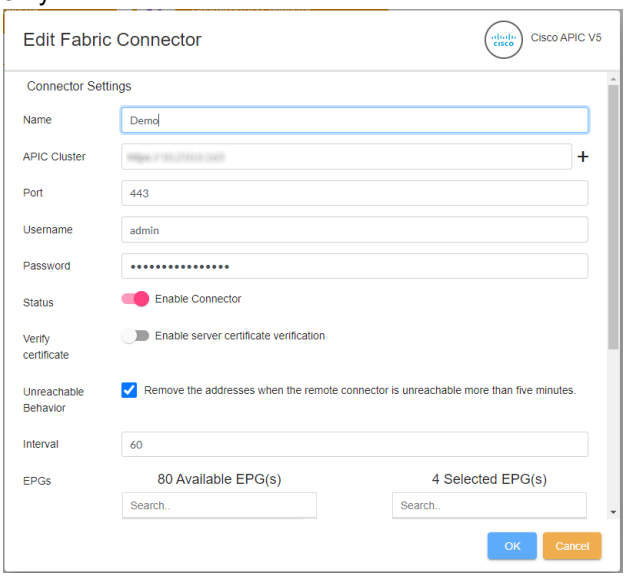
**To create a new Cisco ACI Universal Connector:**

1. Go to *Management Extensions* > *Universal Connector*.
2. Click *Create New* on the toolbar, and select *Cisco ACI*.




3. Enter the connector settings.
4. Click *Save & Continue*, and then set the *Status* toggle to the on position to enable the connector.
5. You can manually enter the update *Interval* for FortiManager to communicate with the Cisco APIC. The default is 60 seconds.

6. FortiManager will authenticate against Cisco APIC using the credentials provided by the administrator on this page. Only once the authentication is successful can the connector can be enabled.

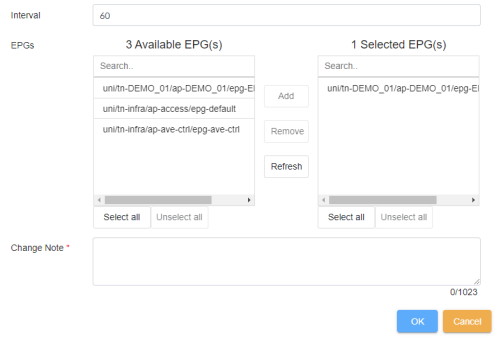



7. You can enable/disable the certificate verification check for the remote Cisco APIC server. The behavior for certificate verification is as follows:
   - If the remote certificate is valid and we enable the certificate verification, login succeeds.
   - If the remote certificate is valid and we disable the certificate verification, login succeeds.
   - If the remote certificate is invalid and we enable the certificate verification, login fails.
   - If the remote certificate is invalid and we disable the certificate verification, login succeeds.

## Importing EPGs from the Universal Connector

**To import EPGs from the connector:**

1. Once the connector is enabled, you can import EPGs and IP address information from the remote Cisco APIC server.
2. All the available EPGs from the server will appear in the *Available* list and can be moved to the *Selected* list for use on the FortiManager.
3. Once moved, enter the *Change Note* and click *OK*.



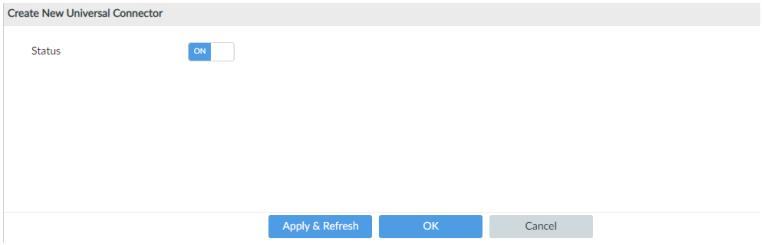

FortiManager will retrieve all the corresponding EPGs and the IP address information from the Cisco ACI server.

## Enabling the Universal Connector

To use the imported EPGs from the connector, administrators will first need to enable the connector.

**To enable the Universal Connector:**

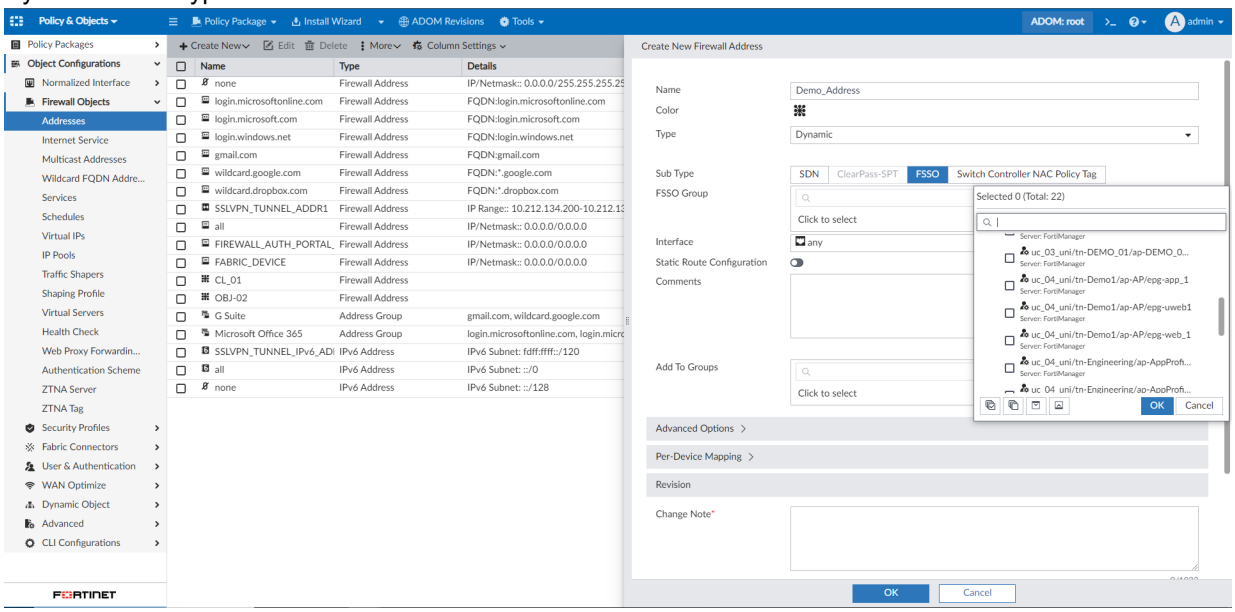
1. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *Endpoint/Identity*.
2. Click *Create New* from the toolbar and select *Universal Connector* from the dropdown.
3. Set the *Status* toggle to the on position to enable the connector.



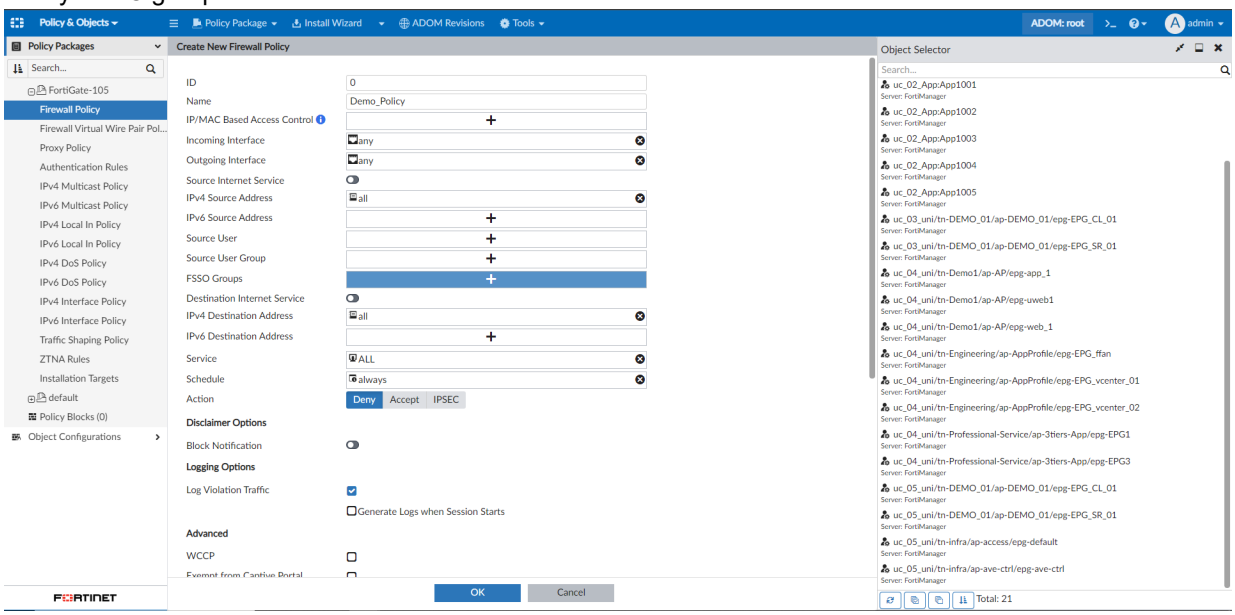

## Using the imported EPGs

The imported labels from the remote host are available as FSSO adgrp, and are selectable in the areas indicated below:

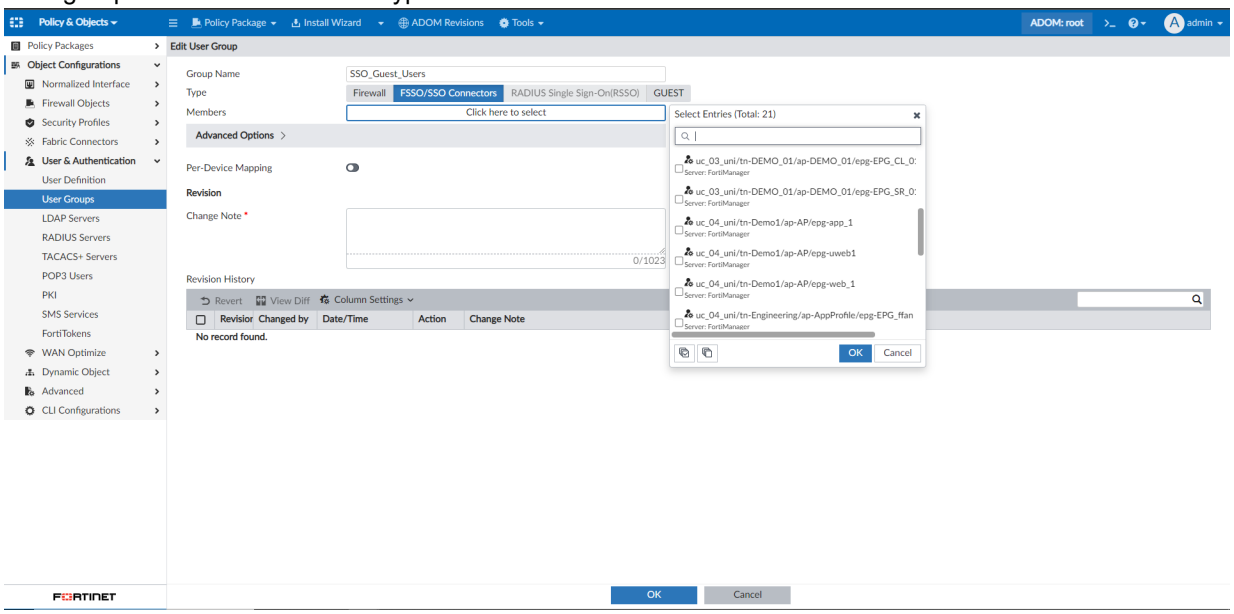
- Dynamic FSSO type address.



- Policy FSSO groups.




- User group FSSO/SSO connector types.

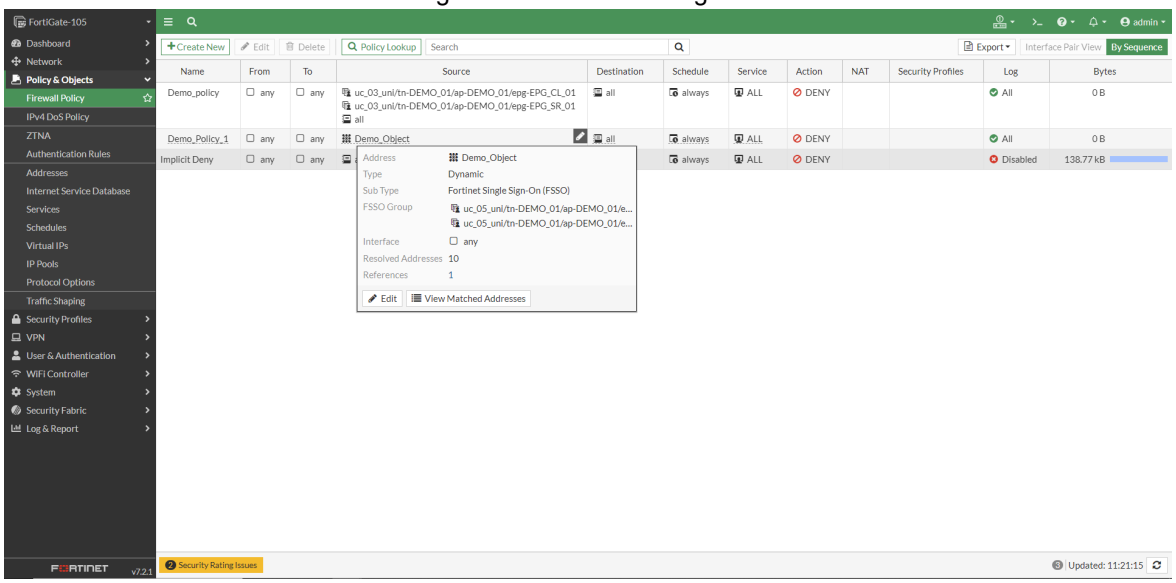


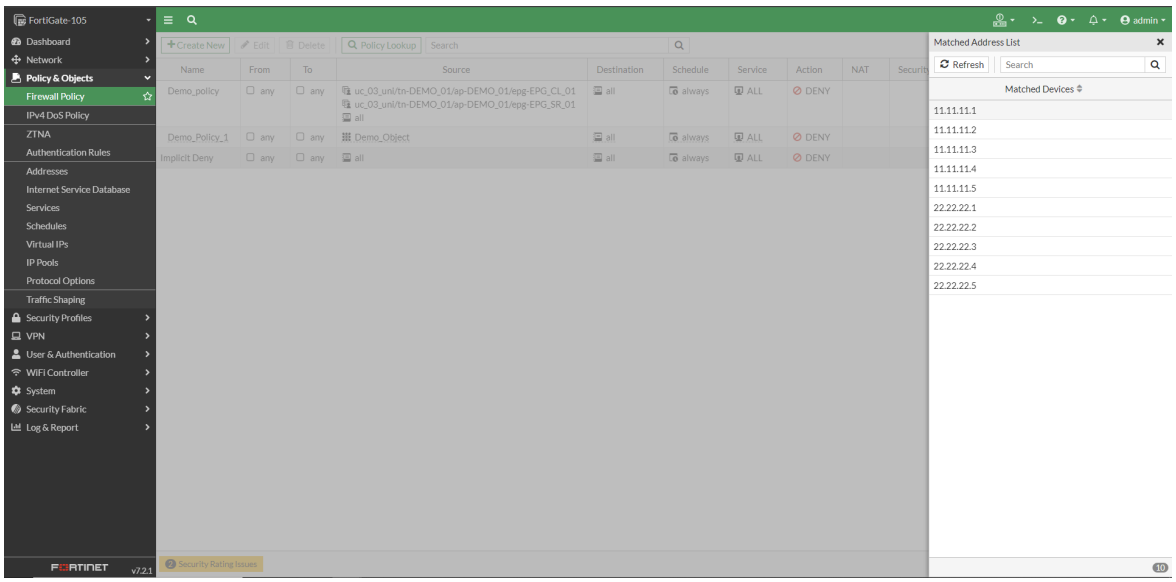

## Cisco ACI connector behavior

1. If the connector is configured but disabled:
   a. In this case, all connectors and FortiManager configurations are still accessible and work, however, the connector does not send any groups and address (corresponding to active sessions) to FortiManager until the connector is enabled.
   b. If the connector was in use but is disabled, the container and FortiManager will maintain all configurations, but address information of active sessions will be removed/cleared.
2. If the connector is configured and functional, but is deleted:
   a. All existing groups information and address information (active sessions) will be cleared from FortiManager/Connector/FSSO/FortiOS.

**b.** If the EPGs are in use in Policy and or Address Objects, these FSSO groups will be stuck on FortiManager. Administrators will need to make sure that all the EPG groups in use should be deleted before deleting the connector.

- If the connector to Cisco APIC is lost after five minutes, action is taken based on whether the administrator has checked the *Remove the address when the connector is unreachable more than 5 minutes* option. This option is enabled by default, and addresses are cleared if the connection to Cisco APIC is lost for five minutes. When the checkbox is not selected, all address information is maintained until the connection is reestablished or the administrator changes the connector configuration.



# Cloud Services

This section lists the new features added to FortiManager for cloud services:



## Automatic configuration synchronization for the members of the auto-scaling group in Public Cloud in case of scale-out/scale-in events - 7.2.1

FortiManager supports automatic configuration synchronization for the members of the auto-scaling group in Public Cloud in case of scale-out/scale-in events.

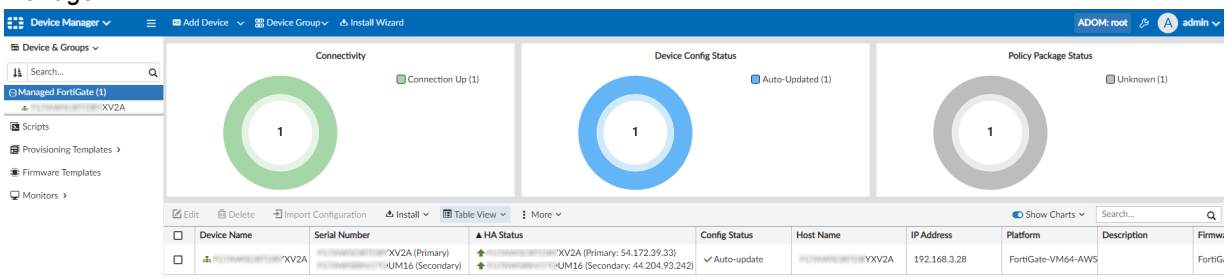
As an example, an administrator creates an auto-scale cluster on the public cloud with two FortiGate-VMs which includes a rule to trigger a scale-out event when the CPU or network utilization exceeds 70% capacity. The scale-out event increases the number of FortiGate-VMs in the cluster to three so that the additional traffic can be managed. In the event of a scale-out, the newly added FortiGate device syncs with the Primary FortiGate in the cluster and fetches the FortiManager configuration. Once the deployment and sync is complete on the new FortiGate, the device is authorized and added to the existing cluster on the FortiManager.

A separate rule specifies that when the CPU or network utilization is less than 10%, a scale-in event occurs to reduce the number of FortiGate-VMs back to two. When the scale-in event occurs, the third FortiGate device is automatically removed from FortiManager. These changes are reflected on the FortiManager without any manual intervention required.

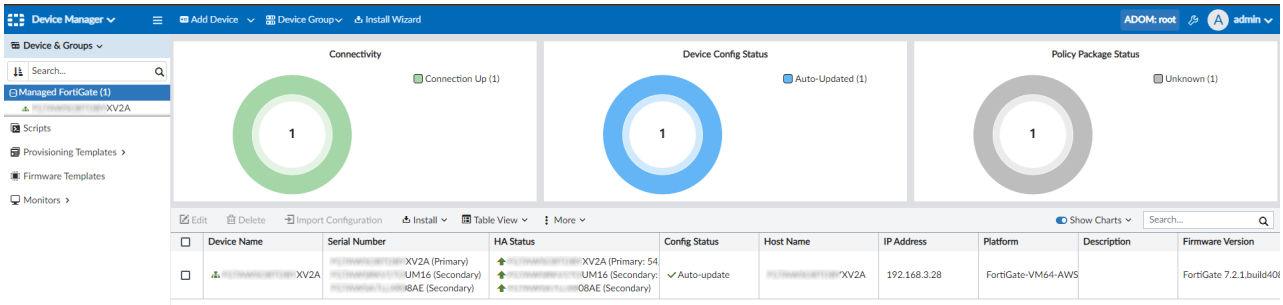
**To manage FortiGate auto-scale clusters on FortiManager:**

1. Add the auto-scale cluster to FortiManager:
   - Add the FortiGate auto-scale cluster to FortiManager for the first time using the IP address of the Primary FortiGate. Once the configuration between the cluster members are in sync, the remaining devices are added to the FortiManager automatically.
   - Alternatively, you can configure the FortiManager Fabric Connector on the Primary FortiGate to add the cluster to FortiManager.

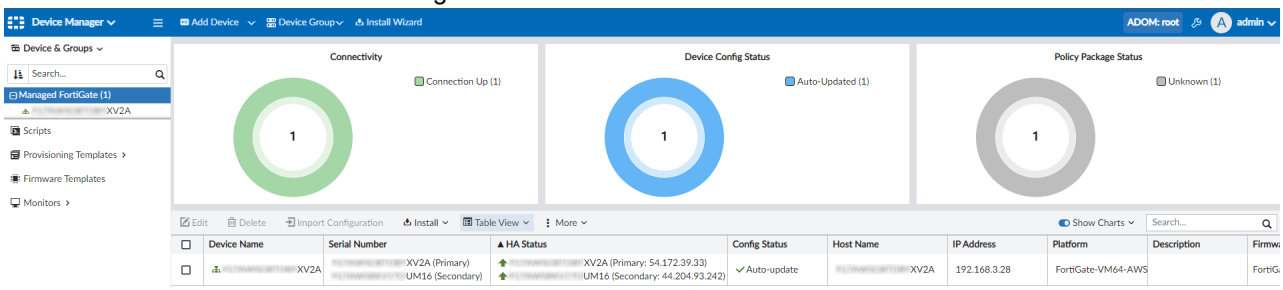
- You can check the *Serial Number*/*Hostname* and *HA Status* of the FortiGate cluster devices in the *Device Manager*.



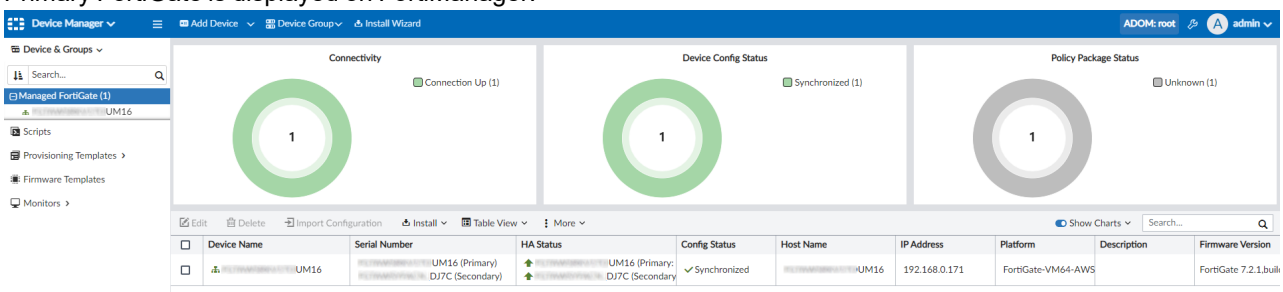

2. When a scale-out event occurs where the number of FortiGate devices in the cluster increases, once the newly added FortiGate becomes a part of the cluster and syncs its configuration with the cluster's Primary device, it is added to FortiManager.
   On FortiManager, the device is automatically authorized and added to the existing cluster without manual intervention.




3. When a scale-in event occurs where the number of FortiGate devices in the cluster decreases, once the FortiGate is removed from the cluster on the cloud and the FGFM expires on the FortiManager, the FortiGate device will be removed from the cluster on FortiManager.




4. During any scale-in event, if the Primary FortiGate is removed from the cluster on the cloud, then FortiManager will be able to detect the change and will reflect the state of the new Primary and Secondary devices in the Device Manager.
   In the example image below the Primary FortiGate failed and there was an auto-scale event to replace it. The new Primary FortiGate is displayed on FortiManager.

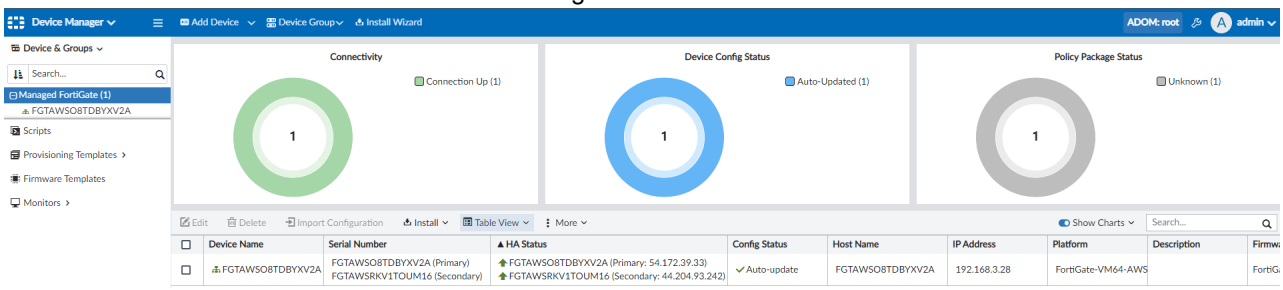


# Visibility improvement for auto-scaling clusters - 7.2.1

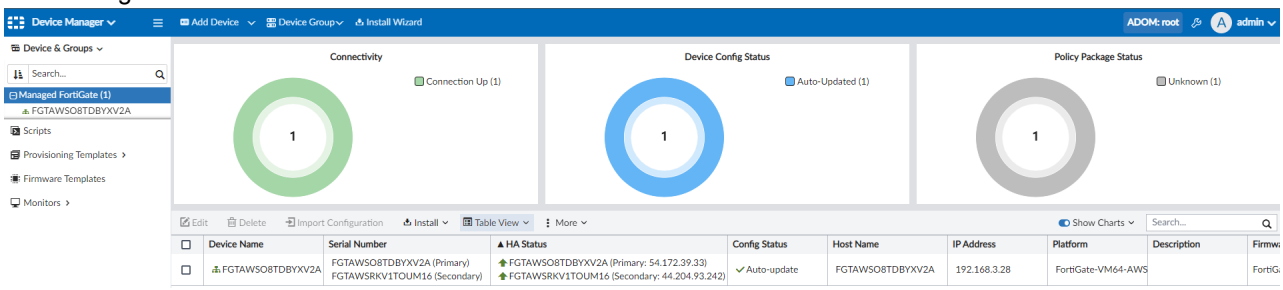
Visibility improvement for auto-scaling clusters with auto-scale status, cluster type, HA status and mode, and elastic IP information of the cluster members.

When viewing auto-scale cluster devices in FortiManager, you can find the following information.

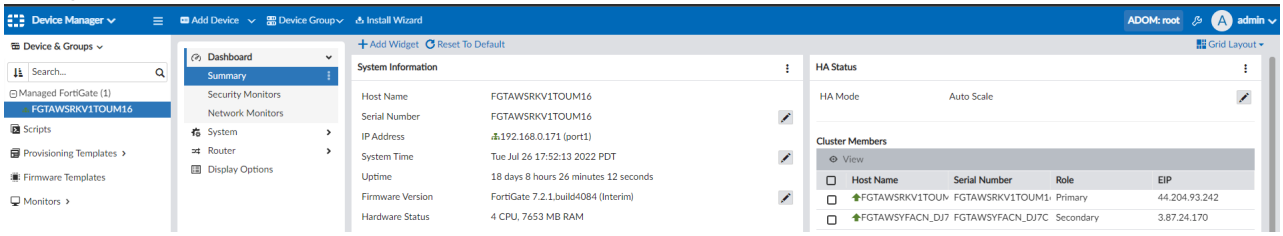
1. Serial number and auto-scale status:
   Administrators can check the serial number and corresponding status (Primary/Secondary) of each member FortiGate in the cluster from the FortiManager.




2. HA status and elastic IP address:
   Administrators can check the HA status and the elastic IP address of each member FortiGate in the cluster from the FortiManager.




3. HA mode and cluster members:
   Administrators can check the HA mode (auto-scale) along with cluster members, roles, and elastic IP in the *Device Manager*.




See also Automatic configuration synchronization for the members of the auto-scaling group in Public Cloud in case of scale-out/scale-in events 7.2.1 on page 234.

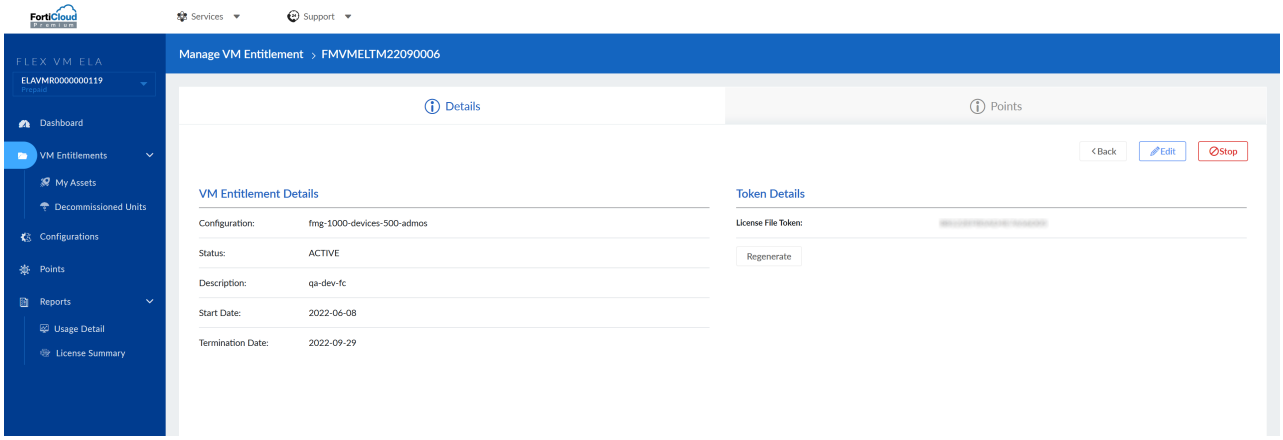
# FortiManager-VM has been added to the Flex-VM offering - 7.2.1

FortiManager-VM has been added to the Flex-VM offering to allow scaling up/down managed FortiGates or number of ADOMs at any given time.

For additional information, see the Flex-VM Administration Guide on the Fortinet Documents library.

**To activate the Flex-VM token:**

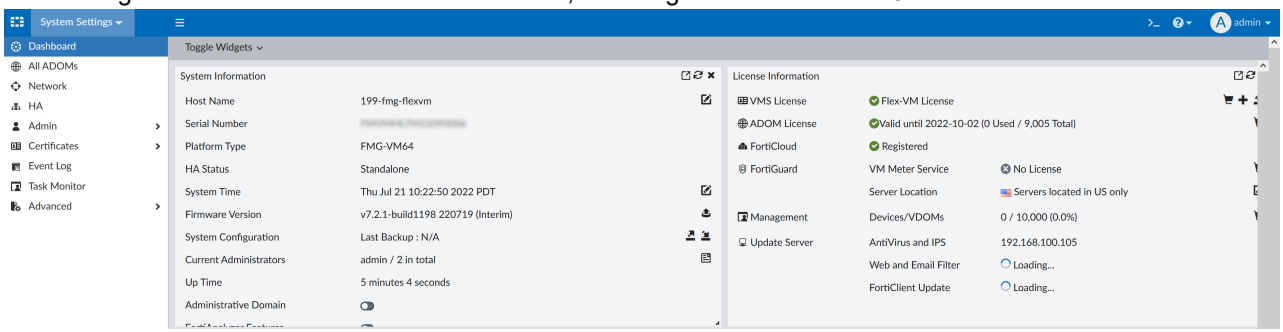
1. In Flex-VM, configure the FortiManager Flex-VM device and ADOM number.




2. Using the FortiManager Flex-VM token, enter the following command in FortiManager to activate the license:

```
execute vm-license <license-token>
```

3. FortiManager will retrieve the license from Flex-VM, including the device and ADOM number.




# VM flexible shapes support for Oracle Cloud Infrastructure - 7.2.1

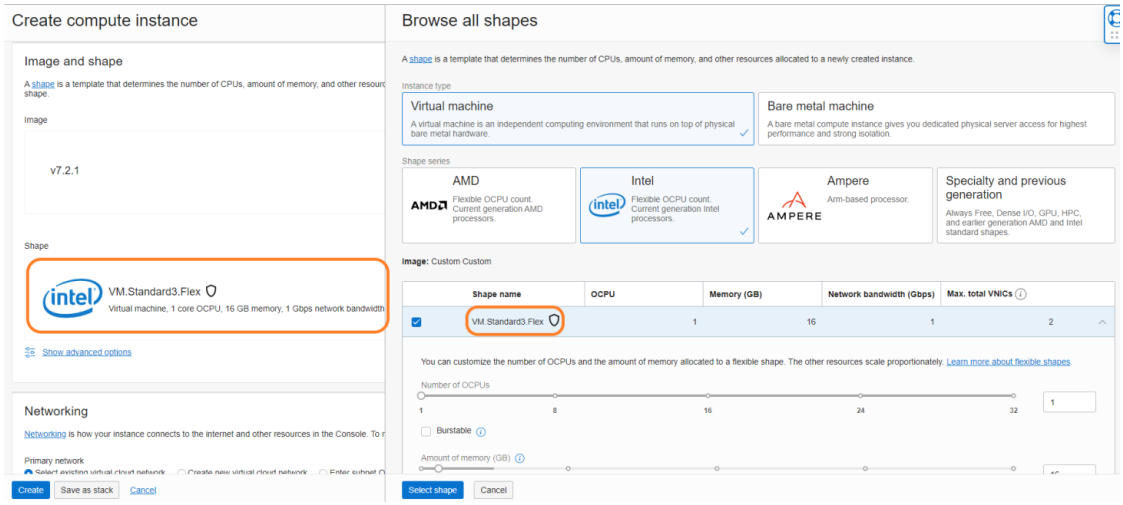
The VM flexible shapes now supported for Oracle Cloud Infrastructure (OCI) permit customization for OCPU and memory resources.

When you create a VM instance using a flexible shape, you can select the number of OCPUs and the amount of memory that you need for the workloads that run on the instance. The network bandwidth and number of VNICs scale proportionately with the number of OCPUs.

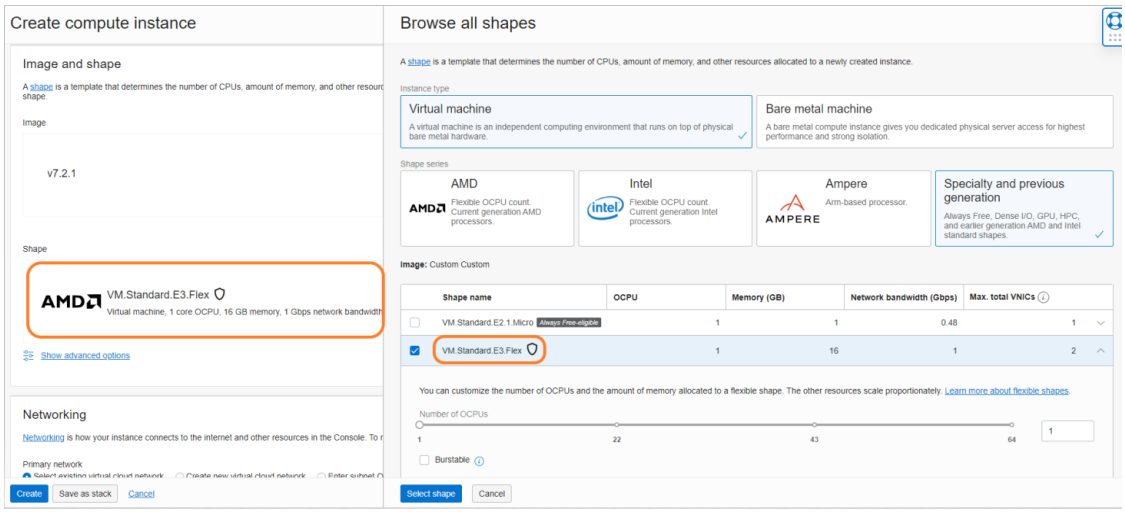
For more information about instance type support, see the FortiManager OCI Administration Guide.

When creating a FortiManager-VM or FortiAnalyzer-VM instance in OCI, you can select one of the following flexible shapes:

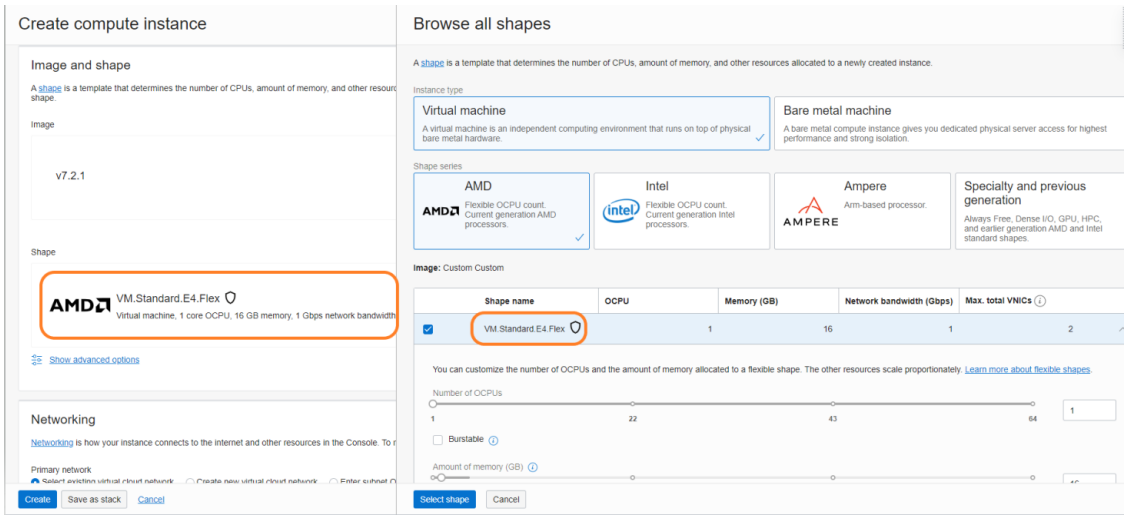
- VM.Standard3.Flex (Intel)




- VM.Standard.E3.Flex (AMD)



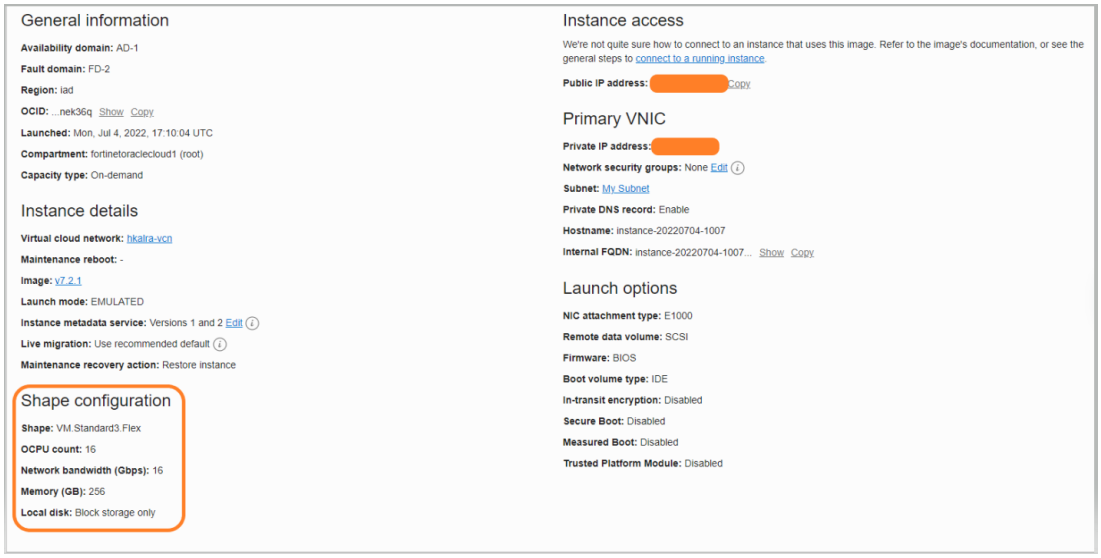

- VM.Standard.E4.Flex (AMD)



When creating an instance with a flexible shape, you can use the horizontal scrolls to customize the *Number of OCPUs* and the *Amount of memory (GB)*.

VM BYOL licenses are based on vCPUs. The minimum vCPU support for FortiManager-VM and FortiAnalyzer-VM is 4. 1 OCPU equates to 2 vCPUs. Ensure that you meet the requirements for your license.

Once the instance is created, you can check the instance shape from the dashboard as well. For example, see the dashboard for a VM.Standard3.Flex (Intel) shape below.



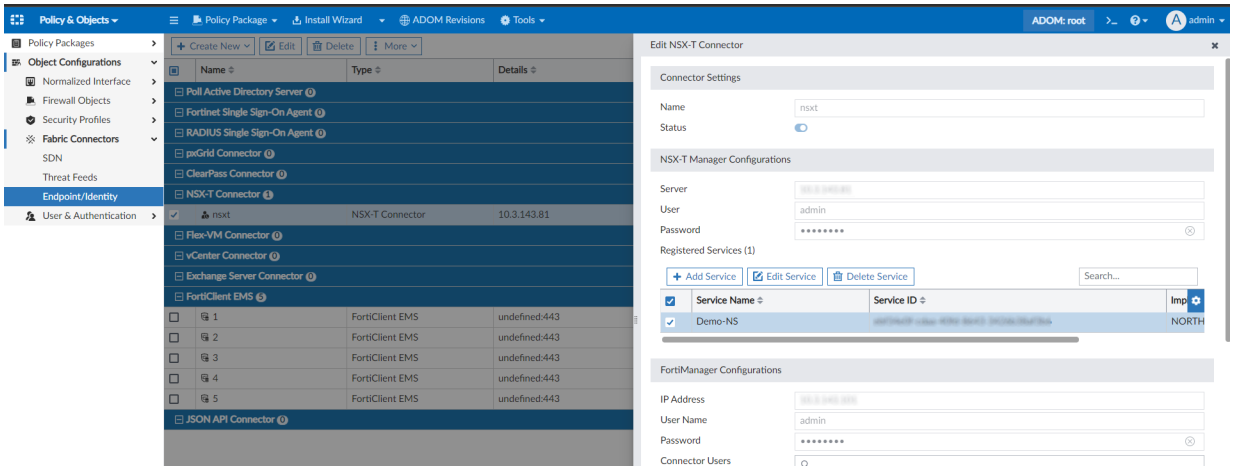

With this flexible shape, you can customize the number of OCPUs and the amount of memory when launching or resizing your VM.

## NSX-T connector options can be managed from FortiManager - 7.2.2

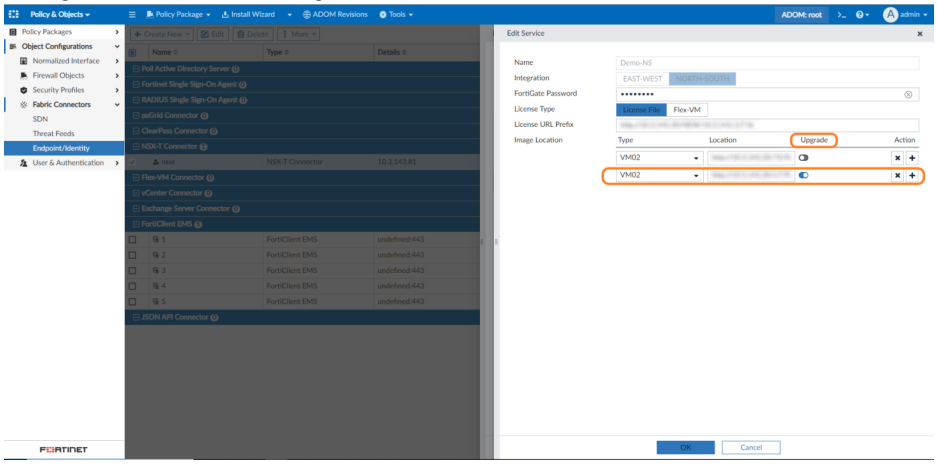
NSX-T connector options can be managed from FortiManager: password, license type, license URL (when used), image location, and update services for deployment specs.

**To edit a registered service:**

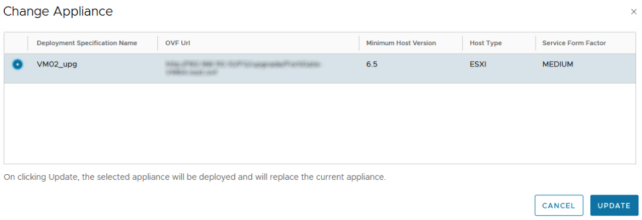
1. Navigate to the NSX-T Connector in FortiManager.
2. Select the Service, and click *Edit Service*.




3. Once Edit Service is selected, the admin is able to change the following information:
   - Password
   - License type
   - License URL (if license type is *License File*)
   - Image location of existing deployment specs
     When upgrading, make sure to mark the change as upgrade by enabling the *Upgrade* toggle. This marks the change on the NSX-T Manager.




Once a deployment spec is set as *Upgrade*, users can upgrade a service deployment using the NSX-T Manager GUI.

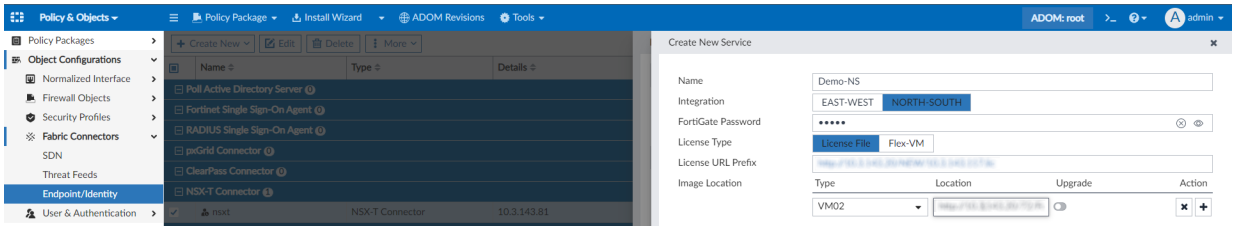


# NSX-T connector support for retrieval of North-South service objects - 7.2.2

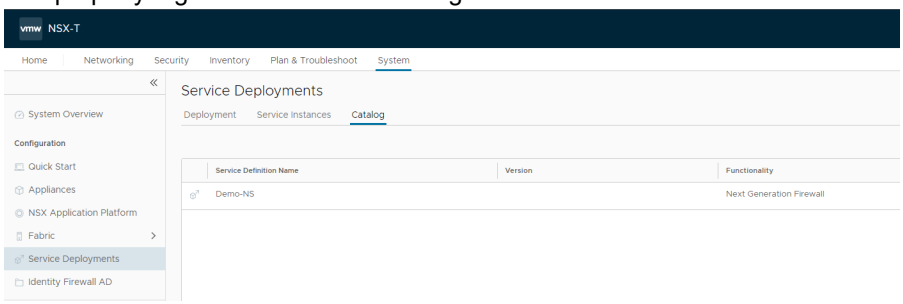
NSX-T connector support for retrieval of North-South service objects

**To register a North-South service:**

1. In FortiManager, go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *Endpoint/Identity*.
2. Edit a previously configured NSX-T connector.
3. Under *Registered Service*, click *Add Service*.
4. Select *North-South* and fill in the details.
5. Click *OK* and save the NSX-T connector.

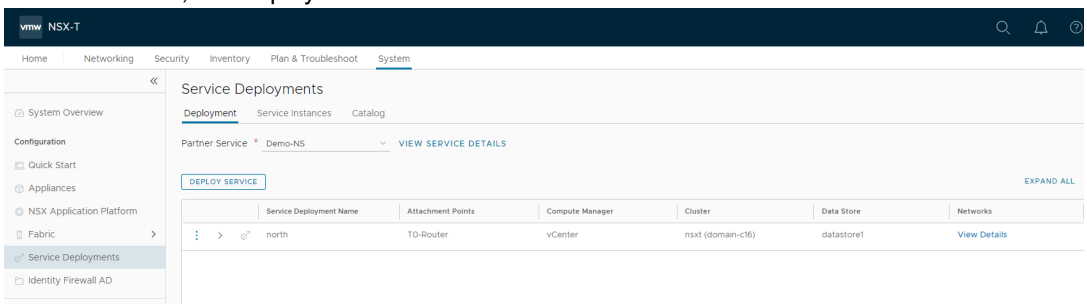



6. In the NSX-T Manager, go to *System* > *Service Deployment* > *CATALOG* to confirm that the FortiGate-VM service was properly registered on NSX-T Manager.



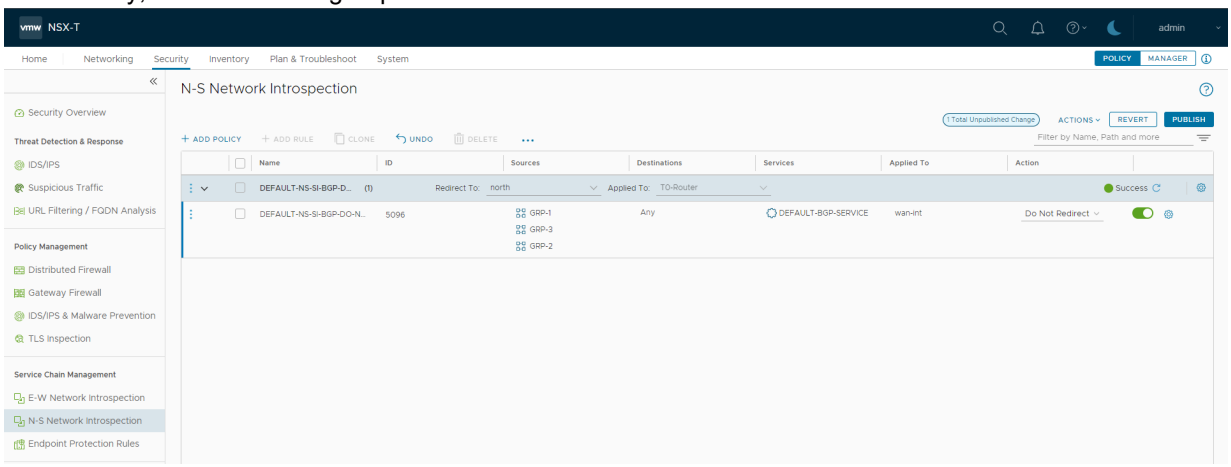

**To deploy a North-South service on NSX-T Manager:**

1. In the NSX-T Manager, go to *System* > *Service Deployment* > *Deployment*.
2. From the dropdown, select the newly registered service and select *Deploy*.
3. Fill in the details, and deploy the service.

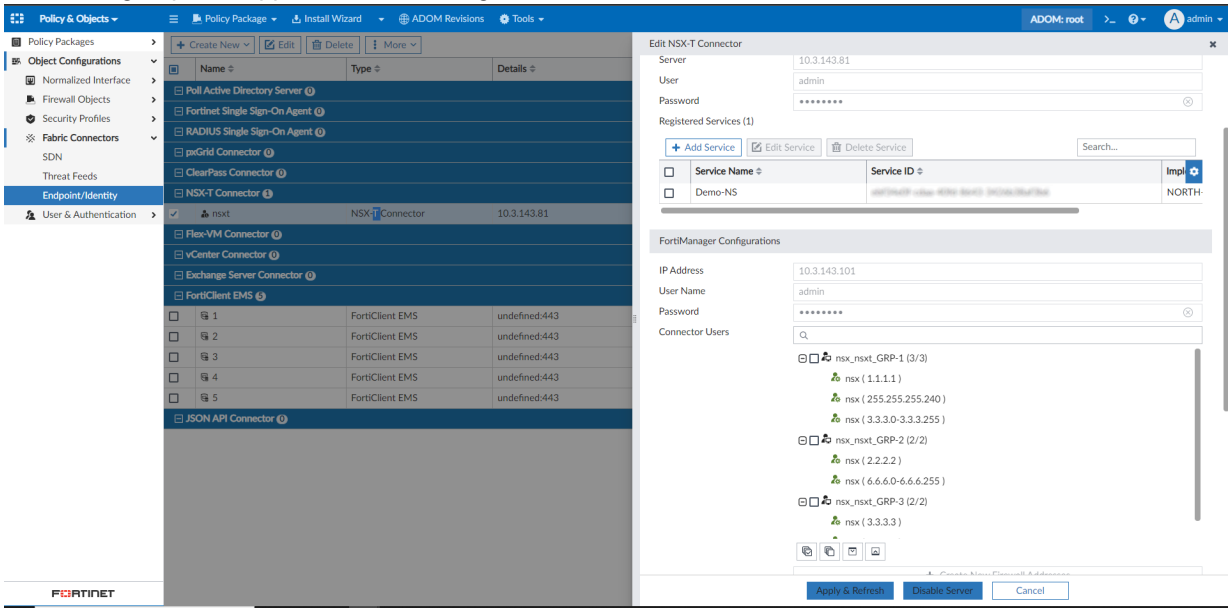


NSX-T currently only supports N-S Introspection once the service is deployed.

4. Associate groups with the North-South service:
   a. Go to *Security* > *Service Chain Management* > *N-S Network Introspection*.
   b. In the Policy, add the desired groups.



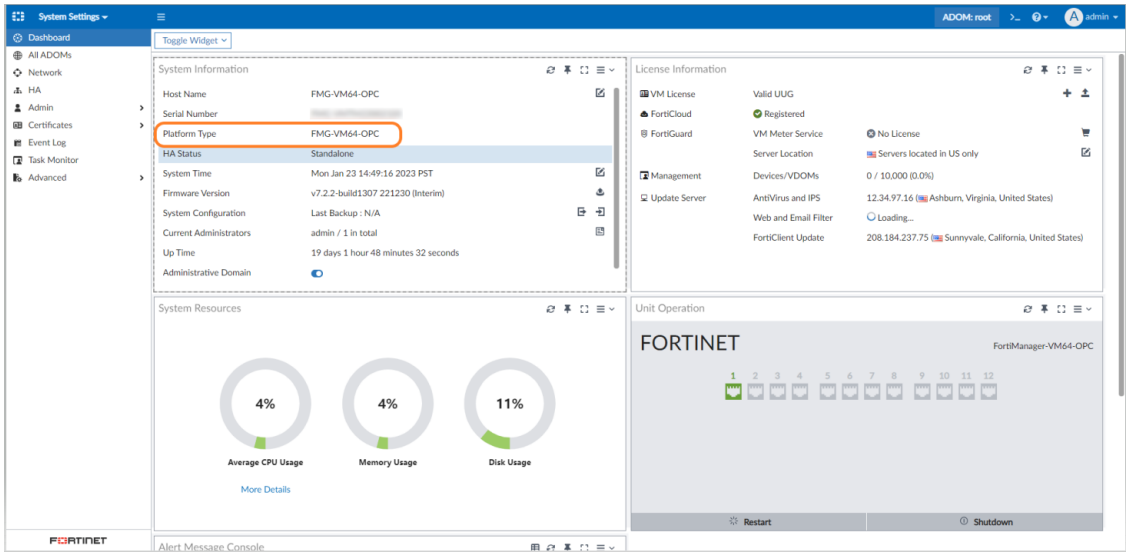

   c. The same groups will appear on FortiManager and be available for use.




# FortiManager-VM added support for Oracle Dedicated Region Cloud - 7.2.2

FortiManager-VM added support for Oracle Dedicated Region Cloud.

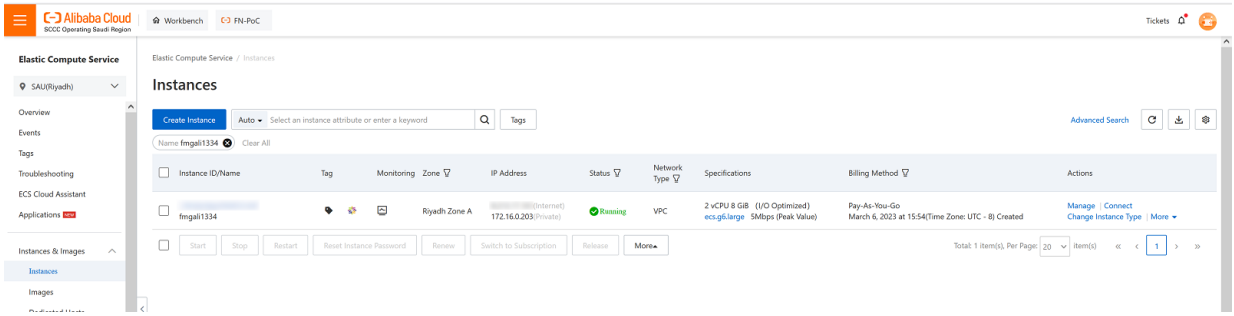
Oracle Dedicated Region Cloud (ODRC) provides all Oracle Cloud Infrastructure (OCI) public cloud services (IaaS/PaaS/SaaS) in a physical location of the customer's choosing. For more information, see OCI Dedicated Region.



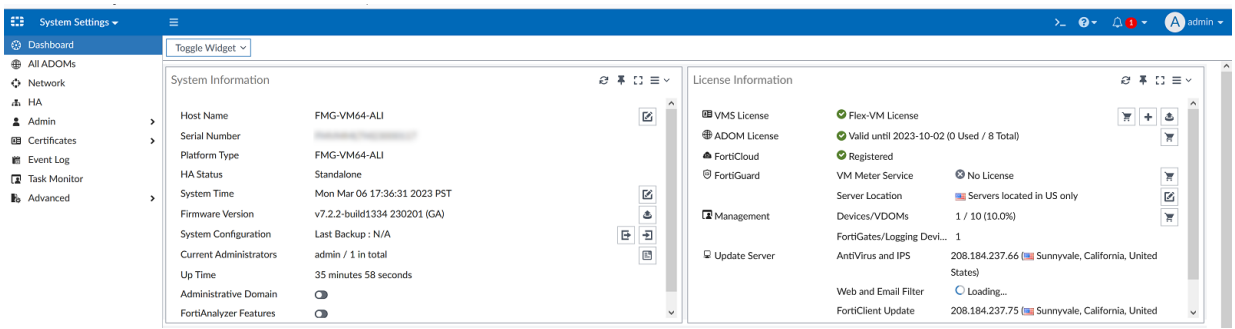

# FortiManager added support for SCCC Alibaba Cloud - 7.2.2

FortiManager added support for Saudi Cloud Computing Company (SCCC) Alibaba Cloud.

- The FortiManager instance is created on SCCC Alibaba Cloud.




- The FortiManager instance using *FMGVM-ALI* functions normally.



# Index

The following index provides a list of all new features added to FortiManager 7.2. The index allows you to quickly identify the version where the feature first became available in FortiManager.

## 7.2.0

## 7.2.1



## 7.2.2

# Appendix A - Example scenarios



## Branch configuration using FortiManager Jinja2 CLI templates

This document provides an example of how deploy model devices for branch FortiGates and configure IPsec/BGP/SD-WAN to connect to the headquarter's HUB FortiGate devices using the FortiManager's Jinja2 CLI templates and template groups.

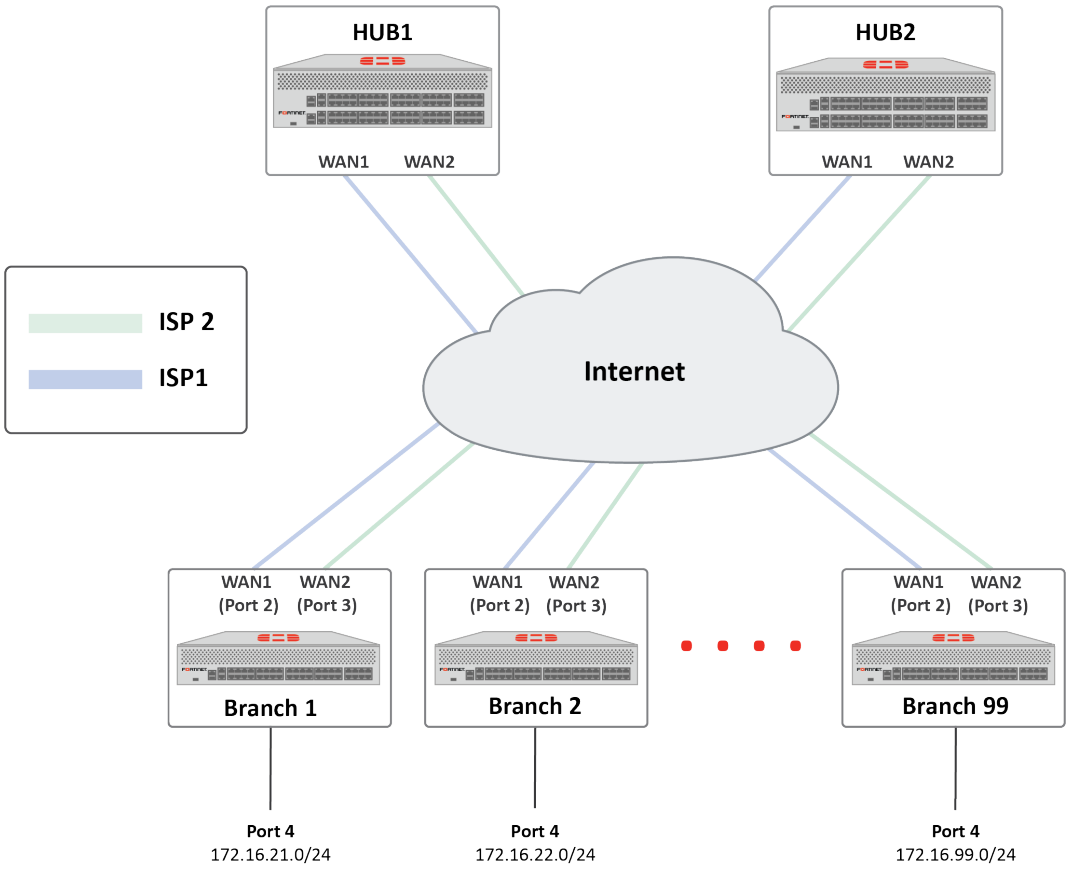
This scenario is not intended as a step-by-step guide, and it is assumed that you have prior knowledge about FortiManager, FortiGate's SD-WAN features, and the Jinja2 language.

This example covers the following:



### Topology

All the provided Jinja2 examples and the configurations used in this example scenario refer to the following topology. Each branch FortiGate has two ISP internet connections (WAN1 and WAN2).



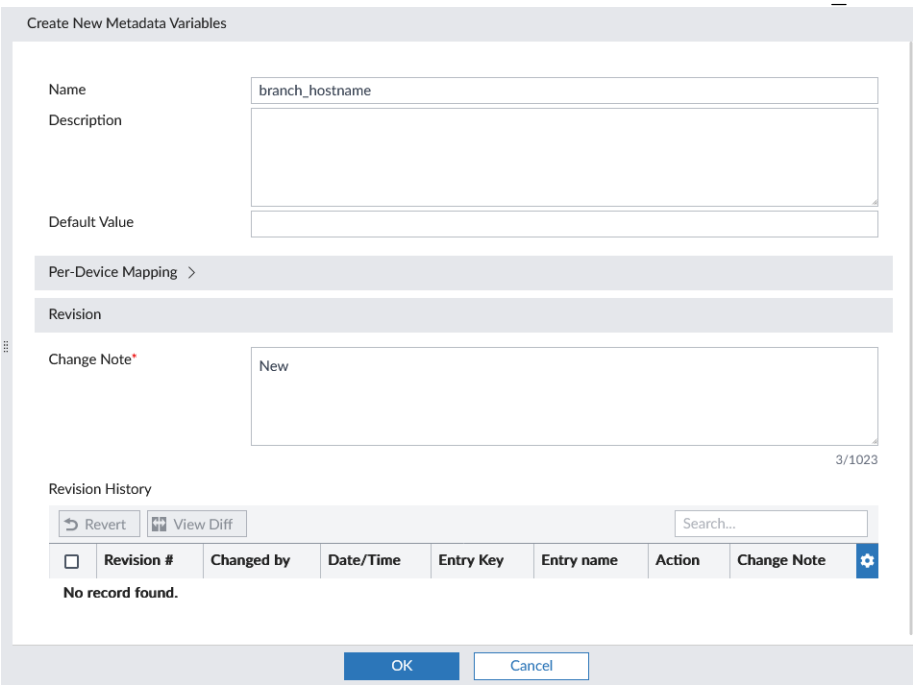

## Create metadata variables used in templates

This configuration uses the following two metadata variables in CLI templates: *branch_hostname* and *branch_id*.

**To create the metadata variables used in the Jinja templates:**

1. Go to *Policy & Objects* > *Tools* > *Display Options*, and select the checkbox beside *Metadata Variables* to enable the option.
2. Go to *Policy & Objects* > *Object Configurations* > *Advanced* > *Metadata Variables*.

3. Click *Create New* to create a new metadata variable with the name `branch_hostname`, and click *OK*.




## Create Jinja templates and a CLI template group

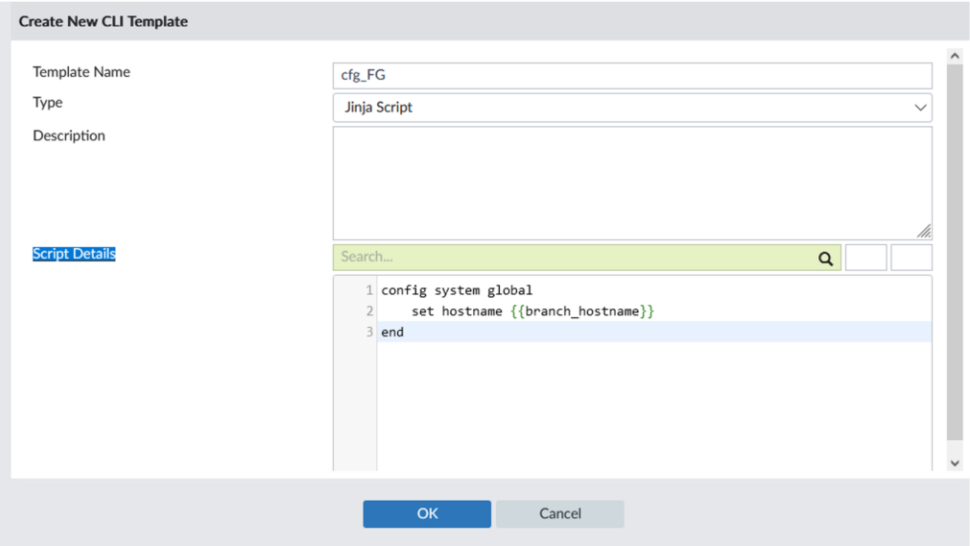
You can create Jinja CLI templates through the Device Manager or by importing a file from your local PC disk. Once the Jinja CLI templates have been created, you can add them all to a CLI template group to simplify management of the templates.

The Jinja CLI templates used in this example can be found inJinja2 template sample scripts on page 260

**To create a Jinja CLI template:**

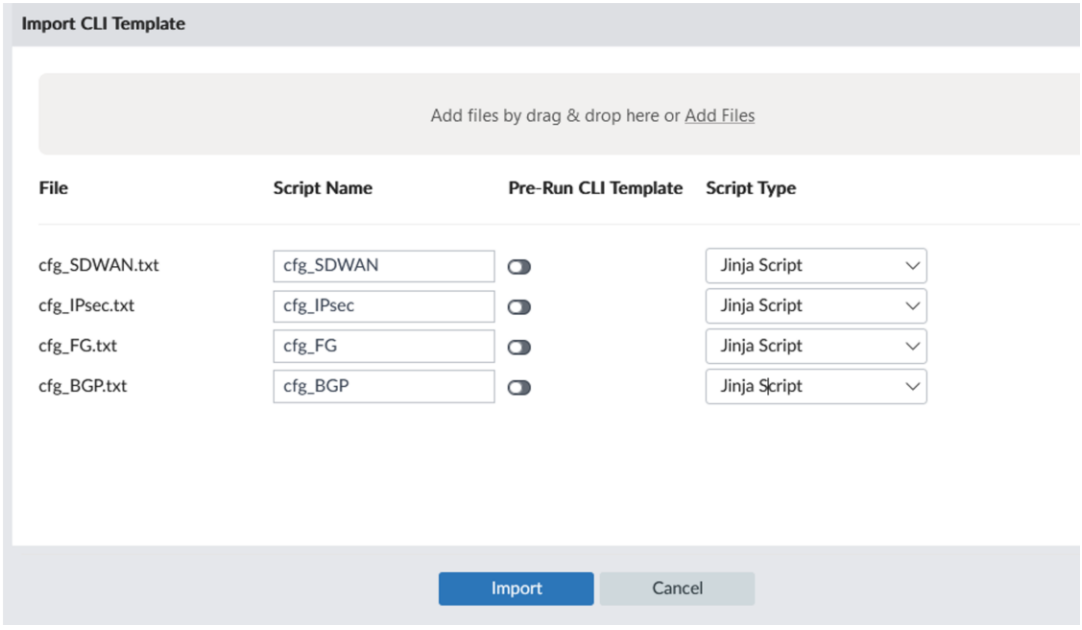
1. Go to *Device Manager* > *Provisioning Templates* > *CLI Templates* > *Create New* > *CLI Template*.
2. Enter the following information, and click *OK*.
   a. *Name*: Enter the name of the template, for example `cfg_FG`.
   b. *Type*: Jinja scripts

c. *Script details*: Input the Jinja script contents.



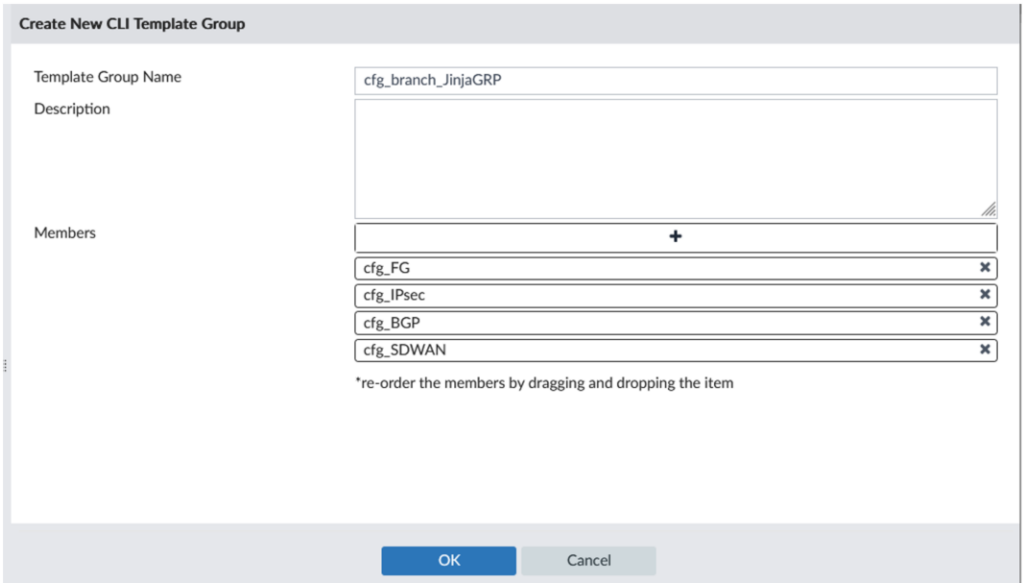

**To import multiple Jinja scripts from a local PC disk:**

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. From the toolbar, select *More* > *Import*.
3. Open the file location on your computer and select the Jinja script files to import. Once the upload is complete, click *Import* to finish.
   In this example, the script name is entered, the *Pre-Run CLI Template* setting is disabled, and the *Script Type* is *Jinja Script*.



**To create a CLI template group:**

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Templates* > *Create New* > *CLI Template Group*.
2. Enter the following information, and click *OK*.
   a. *Template Group Name*: cfg_branch_JinjaGRP.
   b. *Members*: Select the four Jinja templates.
   c. Reorganize the members by dragging-and-dropping them.

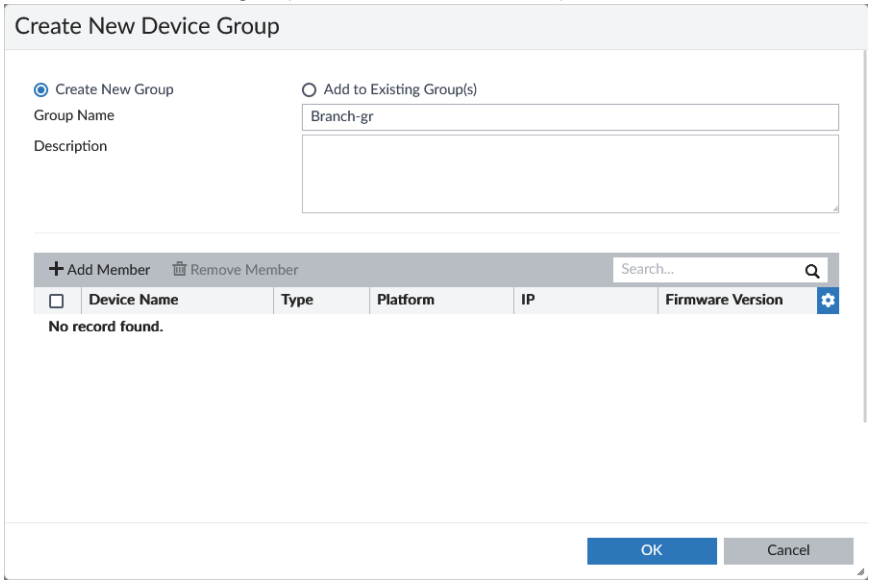



## Create a device group for branch devices

You can create the device group which will include your FortiGate branch devices.

**To create a device group for FortiGate branch devices:**

1. Go to *Device Manager* > *Device & Groups* > *Device Group* > *Create New Group*.
2. Create a new device group with the name *Branch-gr*, and click *OK*.



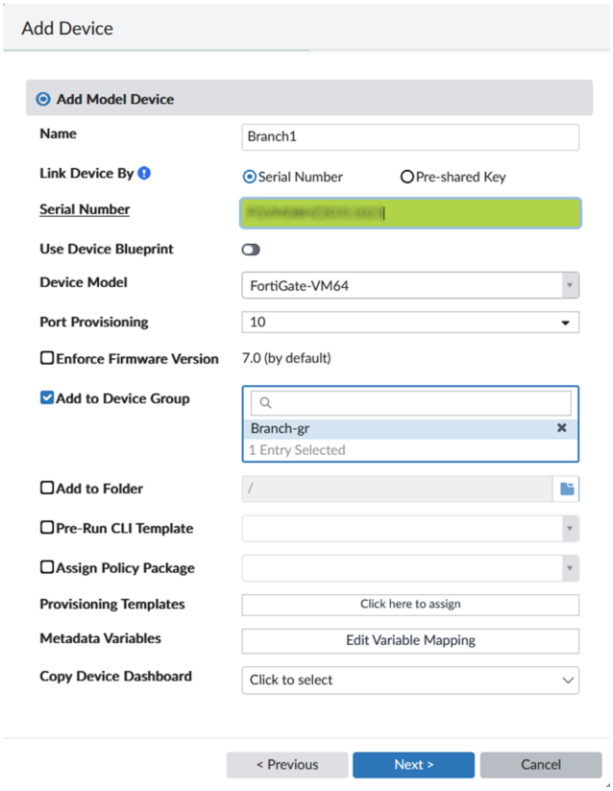

## Create model devices and add them to device group

Create the model devices for your branch devices. Once created, you can add them to the previously configured device group.

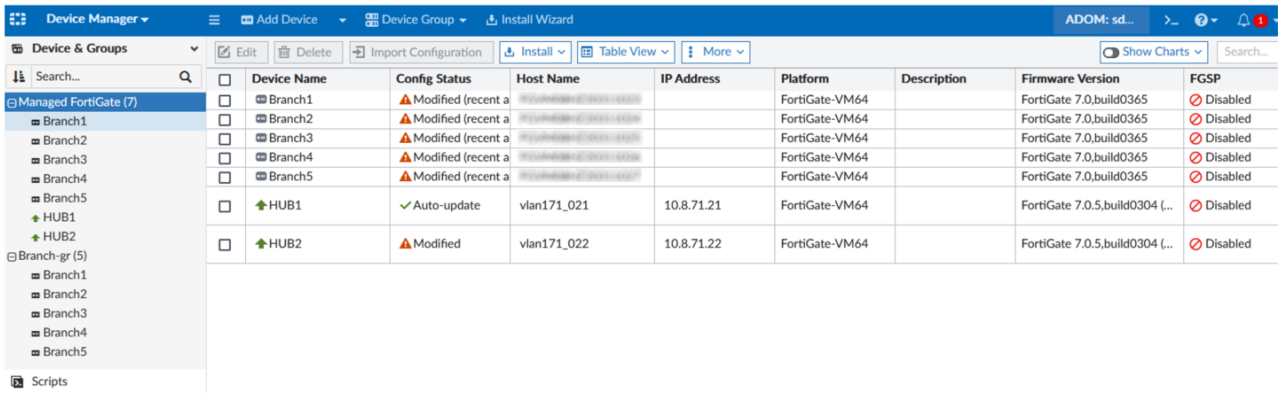
**To add model devices to FortiManager:**

1. Add your FortiGate branch device using the FortiManager Device Manager.
2. Configure the details for your model device, including the device serial number.
   In this example, *Port Provisioning* is configured as 10. FortiManager will create 10 ports for this FortiGate-VM.

3. Enable *Add to Device Group*, and select the previously configured *Branch-gr* device group.




4. Add the other branch models, and view the device manager table to confirm that your devices have been added.

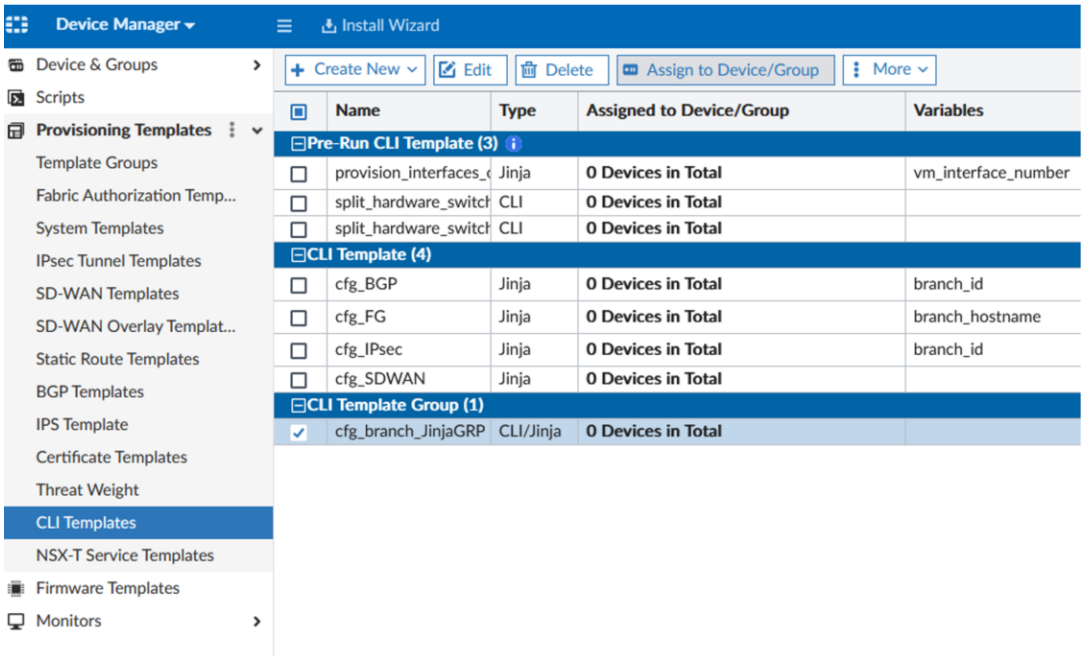



## Assign a Jinja CLI template group to the branch device group

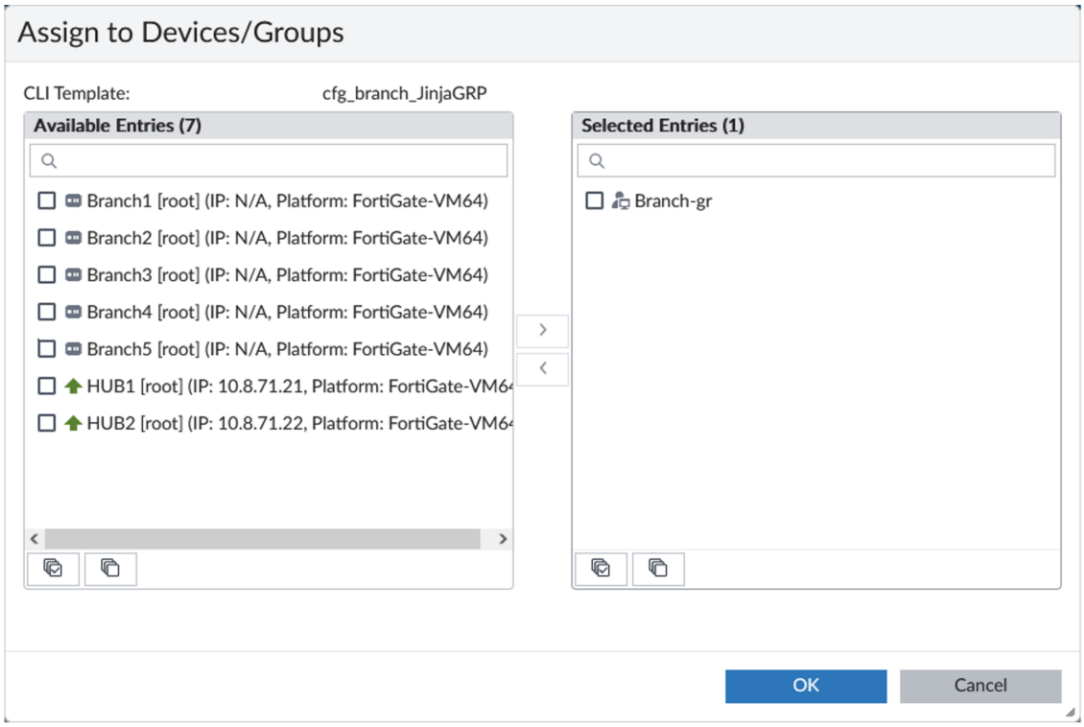
You can assign the Jinja CLI template group which includes your CLI templates to the branch device group.

**To assign the Jinja CLI template group to the branch device group:**

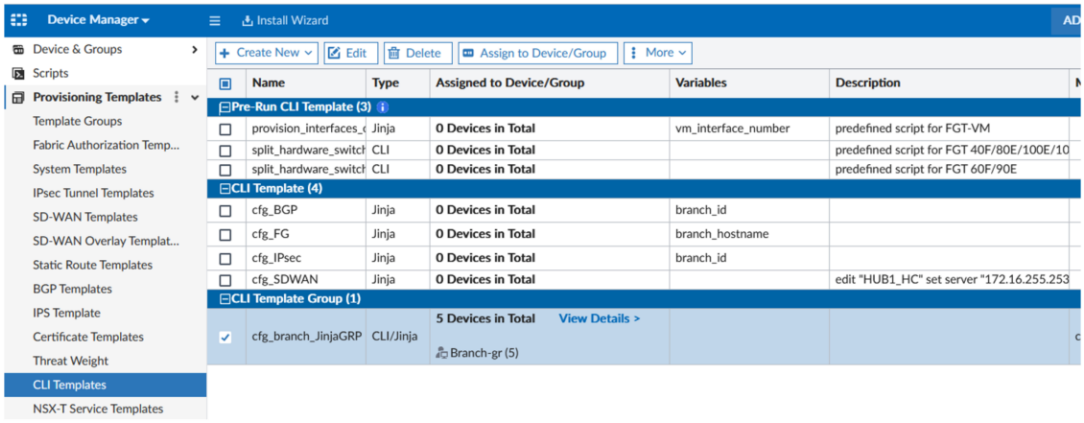
1. Go to *Device Manager* > *Provisioning Templates* > *CLI Templates*.
2. Select the previously created *cfg_branch_JinjaGRP* CLI template group.




3. Click *Assign to Device Group* on the top menu, and select the *Branch-gr* device group.



4. In *Device Manager* > *Provisioning Templates* > *CLI Templates*, the CLI template group has been assigned in the *Assigned to Devices/Group* column.




## Set metadata variable mapping for each branch FortiGate

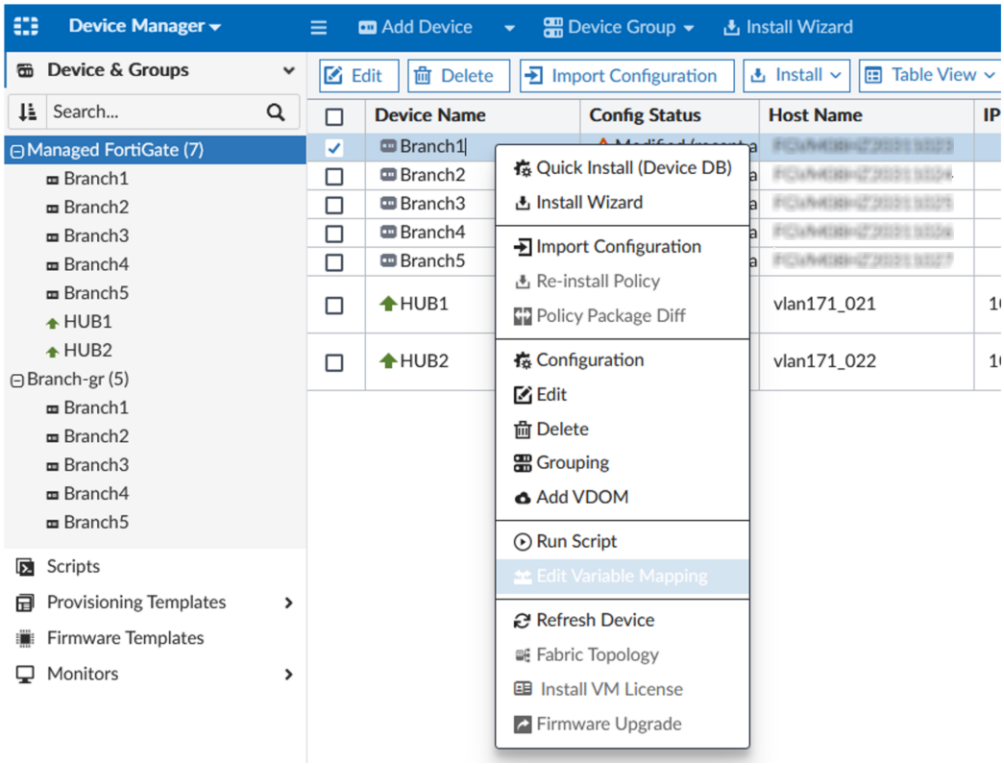
Metadata variable values must be mapped for each branch device.

There are three methods you can use to set values for metadata variables.

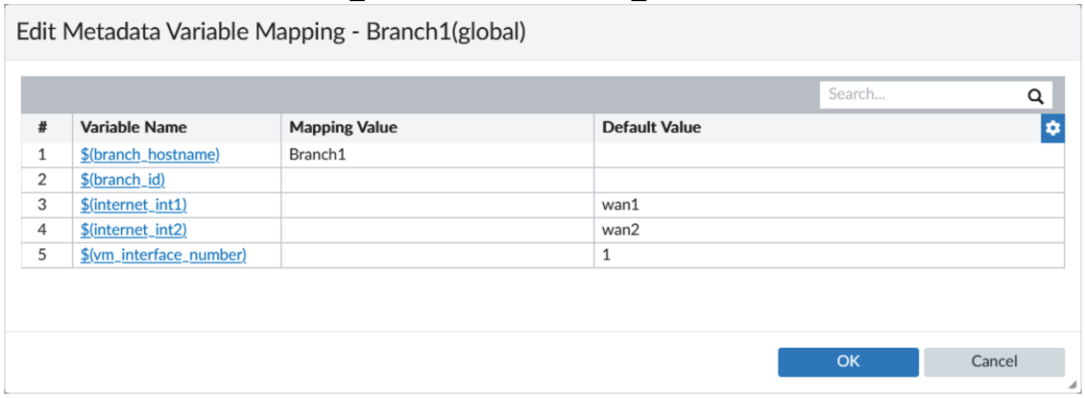
- Editing metadata values from the Device Manager.
- Editing metadata values from Policy & Objects.
- Exporting and importing metadata variables with mappings.

**To edit metadata values in the Device Manager:**

1. Go to *Device Manager* > *Device & Groups*, right-click a device in the device table, and select *Edit Variable Mapping*.




2. Input the values for the `branch_hostname` and `branch_id` metadata variables, and click *OK* to save.

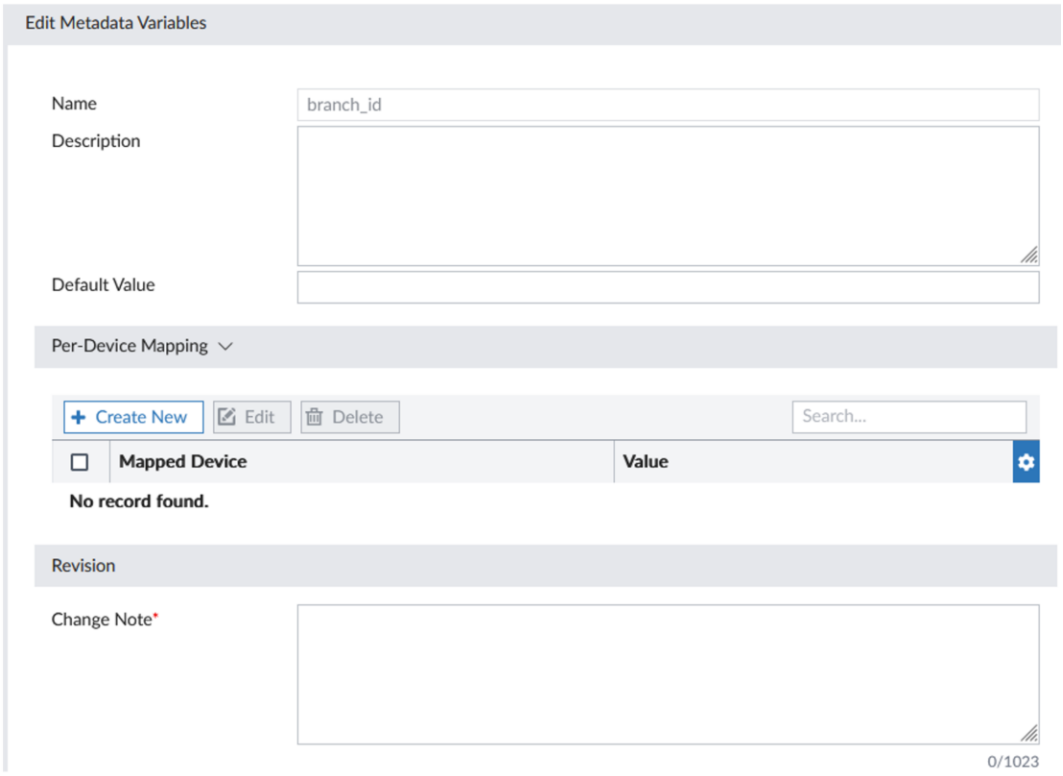



3. Repeat these steps for each model device.

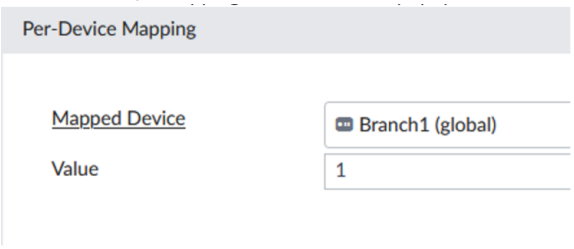
**To edit metadata values in Policy & Objects:**

1. Go to *Policy & Objects* > *Object Configurations* > *Advanced* > *Metadata Variables*.
2. Edit a variable.

3. Click *Create New* under Per-Device Mapping.



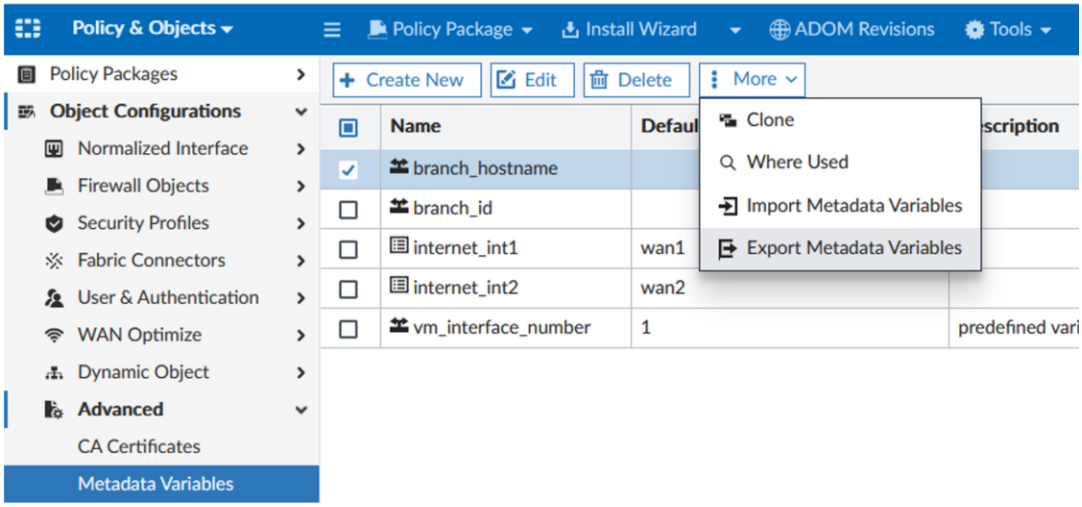

4. Select a mapped branch device and specify the variable value, and click *OK*.
In this example, the model device does not have VDOMs enabled.




5. Repeat this process for each device.

**To export and import metadata values:**

1. Go to *Policy & Objects* > *Object Configurations* > *Advanced* > *Metadata Variables*.
2. Click *More* > *Export Metadata Variables* from the toolbar.




The `metadata_variables.json` file will be downloaded to your computer's Downloads folder. You can edit the JSON file to set values directly by using an external editor.

3. Once the file has been edited, you can import the file back into FortiManager by going to *Policy & Objects* > *Object Configurations* > *Advanced* > *Metadata Variables*, and selecting *More* > *Import Metadata Variables* from the toolbar.

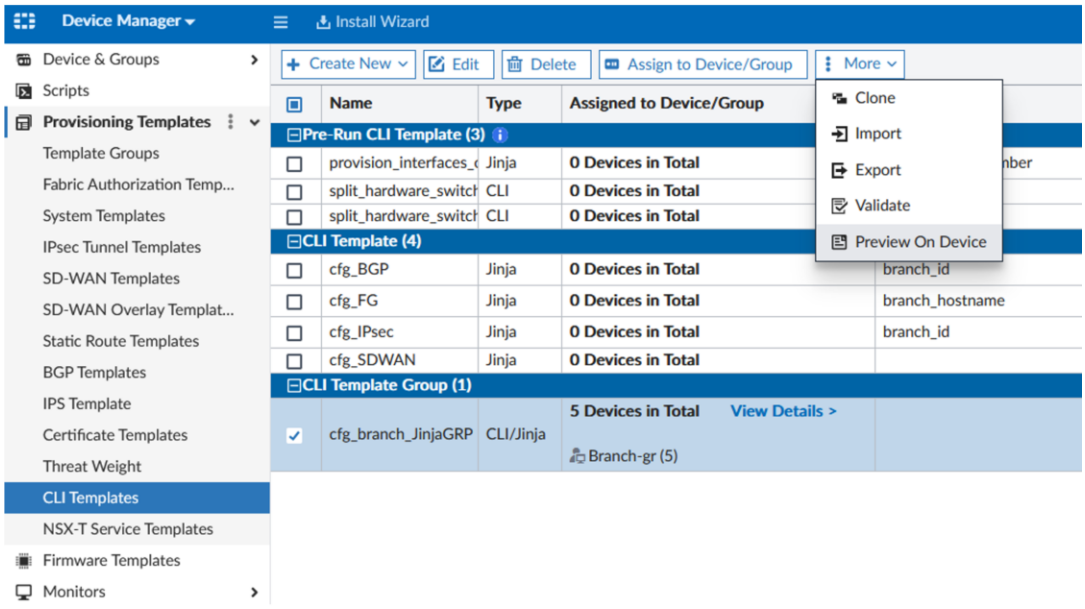
## Preview Jinja script on device or device group

You can preview the Jinja script on a FortiGate device or device group to view the rendered Jinja script contents. If everything looks correct, you can then perform the installation to apply the template to the device.

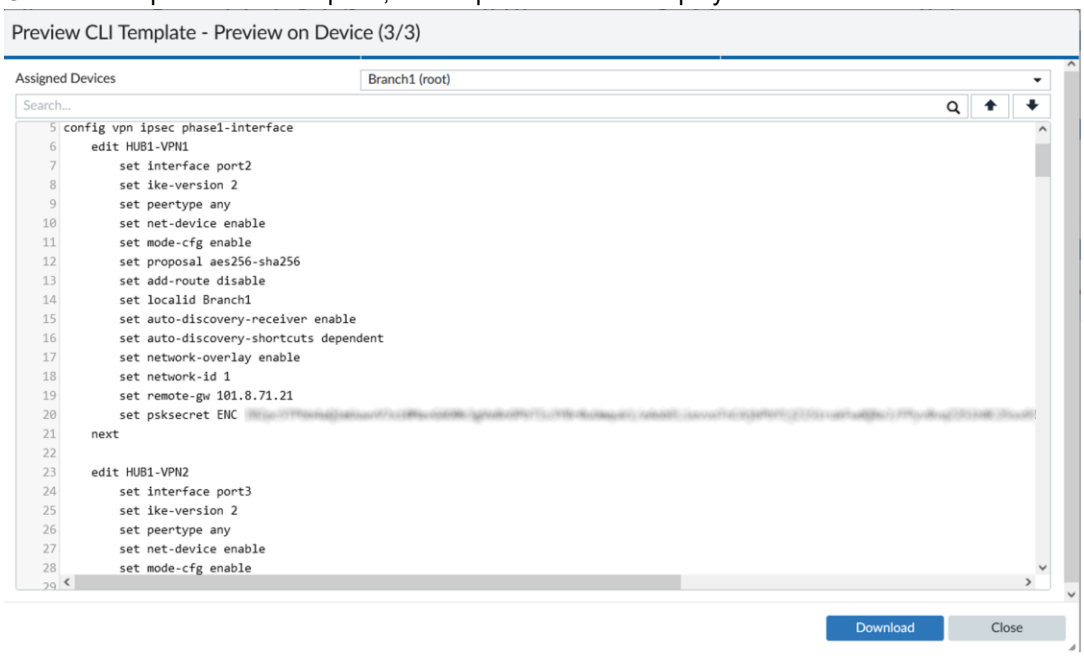
**To preview a Jinja script on a device or device group:**

1. Go to *Device Manager* > *Provisioning Templates* >*CLI Templates*.
2. Under CLI Template Group, select the template group.

3. Click *More* > *Preview On Device* from the toolbar.




Once the script render is complete, the script contents are displayed.



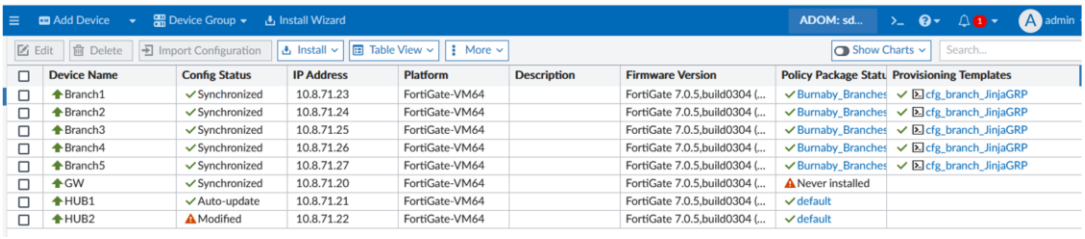

## Perform installation to apply Jinja template configurations to branches

To apply the CLI Jinja templates, you can install the changes to your branch devices.

**To apply the Jinja templates through installation:**

1. Go to *Device Manager* > *Devices & Groups*.
   The *Provisioning Templates* column shows the *cfg_branch_JinjaGRP* is assigned to the branch devices. The yellow caution icon indicates that new changes are not yet applied to the FortiGate devices.

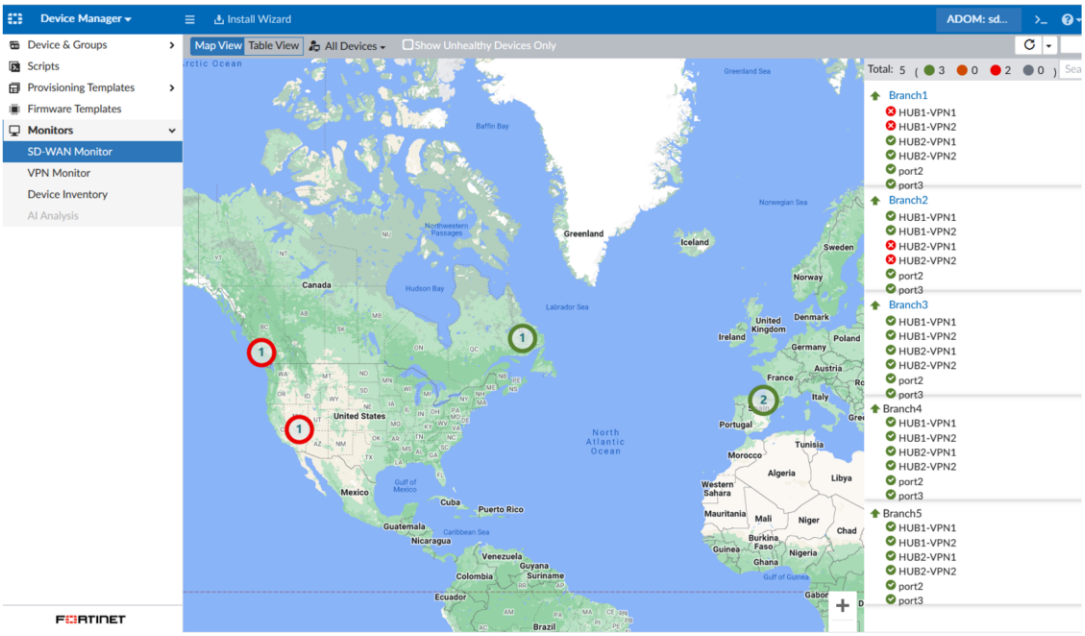
2. Apply the Jinja template to the model devices by performing an installation to the devices.
   There are two options for performing an install.
   - Perform a *Quick Install* from the device database.
   - Install the policy and package and device settings through the *Install Wizard*.
3. Once the ZTP process is finished, you can see the branch FortiGate devices are converted into the real devices with fully synchronized configurations.




You can now view the devices in FortiManager's SD-WAN monitor.

**To view the SD-WAN monitor:**

1. Go to *Device Manager* > *Monitors* > *SD-WAN Monitor*.
   The SD-WAN monitor is displayed.




## Jinja2 template sample scripts

Below are the Jinja2 template sample scripts used within this example.

**cfg_FG**

```
config system global
      set hostname {{ branch_hostname }}
end
```

### cfg_IPsec

```
{# define a list of tunnels #}
{%
  set tunnels= [
    {
      'tunnelname':'HUB1-VPN1',
      'remote_IP':'101.8.71.21',
      'network_id':'1',
      'interface':'port2'
    },
    {
      'tunnelname':'HUB1-VPN2',
      'remote_IP':'102.8.71.21',
      'network_id':'2',
      'interface':'port3'
    },
    {
      'tunnelname':'HUB2-VPN1',
      'remote_IP':'101.8.71.22',
      'network_id':'5',
      'interface':'port2'
    },
    {
      'tunnelname':'HUB2-VPN2',
      'remote_IP':'102.8.71.22',
      'network_id':'6',
      'interface':'port3'
    },
  ]
%}


config vpn ipsec phase1-interface
  {%- for tunnel in tunnels %}
    edit {{ tunnel.tunnelname }}
        set interface {{ tunnel.interface }}
        set ike-version 2
        set peertype any
        set net-device enable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set localid Branch{{branch_id}}
        set auto-discovery-receiver enable
        set auto-discovery-shortcuts dependent
        set network-overlay enable
        set network-id {{ tunnel.network_id }}
        set remote-gw {{ tunnel.remote_IP }}
        set psksecret qa123456
    next
  {% endfor %}
end


config vpn ipsec phase2-interface
```

```
  {%- for tunnel in tunnels %}
    edit {{ tunnel.tunnelname }}
        set phase1name {{ tunnel.tunnelname }}
        set proposal aes256-sha256
        set auto-negotiate enable
    next
  {% endfor %}
end

config system interface
  {% for tunnel in tunnels %}
    edit {{ tunnel.tunnelname }}
      set allowaccess ping
    next
  {% endfor %}
End

config system interface
  {% for tunnel in tunnels %}
    edit {{ tunnel.tunnelname }}
      set allowaccess ping
    next
  {% endfor %}
end
```

**cfg_BGP**

```
{# define the neighbors #}
{%
set neighbors= [
  {
    'neighborID':'31',
    'interface': 'HUB1-VPN1'
  },
  {
    'neighborID':'63',
    'interface': 'HUB1-VPN2'
  },
  {
    'neighborID':'159',
    'interface': 'HUB2-VPN1'
  },
  {
    'neighborID':'191',
    'interface': 'HUB2-VPN2'
  },
]
%}

{# define function  build_bgp() #}
config router bgp
    set as 65000
    set router-id 172.16.0.{{branch_id}}
    set ibgp-multipath enable
    set additional-path enable
    set recursive-next-hop enable
```

```
    set graceful-restart enable
    set additional-path-select 4
    config neighbor
       {%- for item in neighbors %}
        edit 10.10.{{item.neighborID}}.253
            set advertisement-interval 1
            set capability-graceful-restart enable
            set link-down-failover enable
               set soft-reconfiguration enable
            set description {{item.interface}}
               set interface {{item.interface}}
            set remote-as 65000
            set connect-timer 10
            set additional-path receive
           next
       {% endfor %}
    end
end
```

### cfg_SDWAN

```
{%
  set zone= [
    {
      'name':"WAN1",
      'member':'port2',
    },
    {
      'name':"WAN2",
      'member':'port3',
    },
    {
      'name':"HUB1",
      'member':'HUB1-VPN1',
    },
    {
      'name':"HUB1",
      'member':'HUB1-VPN2',
    },
    {
      'name':"HUB2",
      'member':'HUB2-VPN1',
    },
    {
      'name':"HUB2",
      'member':'HUB2-VPN2',
    },
  ]
%}

config system global
set hostname {{branch_id}}
end

{# Config SDWAN Zone and Zone Member #}
config system sdwan
```

```
set status enable
config zone
{%- set exclude_zone = [] %}
{%- for item in zone if item.name not in exclude_zone  %}
    {{ exclude_zone.append(item.name) or ""}}
    edit {{ item.name }}
    next
{% endfor %}
end

config members
{%- for i in zone %}
  edit {{ loop.index }}
      set interface {{ i.member }}
      set zone {{ i.name }}
  next

{% endfor %}
end
```

www.fortinet.com